Titre: Title:	Schéma de gestion et contrôle d'admission basés sur des politiques et des mesures pour le domaine à commutation de paquets du réseau coeur d'UMTS
Auteur: Author:	Mélissa Georges
Date:	2005
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Georges, M. (2005). Schéma de gestion et contrôle d'admission basés sur des politiques et des mesures pour le domaine à commutation de paquets du réseau coeur d'UMTS [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8413/

UNIVERSITÉ DE MONTRÉAL

SCHÉMA DE GESTION ET CONTRÔLE D'ADMISSION BASÉS SUR DES POLITIQUES ET DES MESURES POUR LE DOMAINE À COMMUTATION DE PAQUETS DU RÉSEAU CŒUR D'UMTS

MÉLISSA GEORGES
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)

MARS 2005

Your file Votre référence
ISBN: 978-0-494-47665-9
Our file Notre référence
ISBN: 978-0-494-47665-9

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

SCHÉMA DE GESTION ET CONTRÔLE D'ADMISSION BASÉS SUR DES POLITIQUES ET DES MESURES POUR LE DOMAINE À COMMUTATION DE PAQUETS DU RÉSEAU CŒUR D'UMTS

présenté par : GEORGES Mélissa

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. FERNANDEZ José, Ph.D., président

M. PIERRE Samuel, Ph.D., membre et directeur de recherche

M. QUINTERO Alejandro, Doct., membre

REMERCIEMENTS

Je tiens avant tout à remercier mon directeur de recherche Dr Samuel Pierre pour son support et ses conseils exemplaires. Je le remercie également de m'avoir donné l'opportunité d'effectuer un stage au sein de la chaire CRSNG-Ericsson.

Je tiens ensuite à remercier mon superviseur immédiat à Ericsson M. Yves Lemieux pour son support. J'en profite par la même occasion pour remercier ses collègues M. Suresh Krishnan et M. Alan Kavanagh pour leurs critiques constructives.

Je remercie aussi les membres du LARIM pour leur appui ou leurs commentaires opportuns sur ma recherche. Je pense particulièrement à M. Fabien Houeto, Mme Meral Shirazipour, M. Antoine Lemay, M. Racha Ben Ali et Mme Valérie Alandzi.

Finalement, je remercie mes parents, mon frère, ma sœur et mon copain pour leur soutien et leur indulgence tout à fait exceptionnels.

RÉSUMÉ

L'instance de standardisation d'UMTS (3GPP) développe actuellement une approche de gestion fondée sur les politiques des services, une solution qui s'appuie sur le sous-système multimédia IMS. Il en est résulté le mécanisme de contrôle d'admission basé sur des politiques. Néanmoins, des lacunes peuvent être relevées dans le cadre générique de 3GPP sur l'approche de gestion et le module d'intérêt, plus précisément au niveau de leurs volets inhérents de « politique » et de « disponibilité des ressources ». Ce mémoire traite de ces questions et formule des propositions qui se rapportent au domaine à commutation de paquets du réseau cœur d'UMTS.

À partir de la version cinq de normalisation d'UMTS, une gestion fondée sur les politiques des services est exercée afin de faciliter la configuration du système. Elle appuie les efforts des éléments du réseau qui concourent à l'offre de bout en bout de la qualité de service. Cette solution repose sur le sous-système multimédia IMS qui supplémente le domaine à commutation de paquets du réseau de cœur. Mais, si les efforts consacrés à la définition de cette approche sont énormes dans le cadre générique de 3GPP, les volets « politique » et « disponibilité des ressources » sont sujets à améliorations. En ce qui concerne le premier volet, nous pouvons noter les limitations des politiques définies, le nombre limité de nœuds clients de politiques et l'utilisation exclusive de cette forme de gestion pour les applications multimédias.

En ce qui concerne le volet « disponibilité des ressources », il est quasiment non traité dans 3GPP de sorte que la forme de gestion est, selon nous, amputée d'une composante fondamentale à son fonctionnement. Ceci est d'autant plus grave que le trafic de troisième génération possède des composantes d'auto-similarité et de dépendance à long terme. Ces propriétés dans le trafic se traduisent par des fluctuations grandes en amplitude et persistantes sur plusieurs échelles de temps. Elles sont imputables aux différents comportements des usagers et au caractère instable des protocoles adaptatifs ou aux applications elles-mêmes. Ainsi, s'ensuivent l'inadéquation des modèles markoviens, l'invalidation des résultats associés (théorie des files d'attente,

estimations pour le délai, le taux de perte et le débit), la popularisation des distributions à queue lourde, etc. En conséquence, les études recommandent les mécanismes de contrôle d'admission basés sur des mesures parce qu'ils permettent de pallier les incongruités dans le trafic et les changements dans les réseaux UMTS.

À la lumière de ces constatations, nous proposons un schéma de fonctionnement et un mécanisme de contrôle d'admission qui s'appuient sur des politiques et des mesures. Les caractéristiques de la solution globale sont tirées de la vaste littérature et des cadres génériques des instances IETF et 3GPP. Les modifications visent surtout à ébaucher des politiques nouvelles et à enrichir le schéma de gestion avec la connaissance de la disponibilité des ressources. La proposition repose sur des L-LSP pseudo-statiques, un SGSN abritant un client de politiques, un *Bandwidth Broker* hébergeant un manager SNMP, un serveur de politiques et le mécanisme de contrôle d'admission basé sur des mesures AC-MVEv2/AC-KQv2 et, enfin, des entités SNMP dans les GSN qui s'acquittent de la collecte des mesures d'utilisation des LSP. De plus, le sous-système des services IP améliorés (EISS Enhanced IP Services Subsystem) succède au sous-système multimédia IMS. Il se charge des contrats de haut niveau de qualité de service (applications multimédias, usagers importants, etc.). Tout ceci se traduit par la modification des processus d'établissement de session pour les applications sophistiquées et l'addition de certaines fonctionnalités au niveau des éléments du réseau.

Afin d'attester de la qualité de notre solution, quelques expériences de simulation ont été réalisées sur la version 10.5 d'OPNET. La preuve de concept a porté uniquement sur le volet « disponibilité des ressources » et seul l'algorithme AC-MVEv2 a été considéré. Les adaptations de l'environnement de simulation incluent un réseau non UMTS supportant MPLS et DiffServ, des profils de QdS permissifs, des tailles pour les files d'attente et les tampons assez grandes, des niveaux de congestion modérés et, enfin, des mécanismes de conditionnement peu restrictifs vis-à-vis du trafic. Les buts étaient d'identifier le compromis que peut offrir notre solution entre l'utilisation des ressources et la QdS et de le comparer à celui de la solution d'OPNET, une solution similaire à celle de 3GPP sur ce volet en raison de sa faible teneur en mécanismes de QdS. Dans ce

mémoire, il est sous-entendu que la congestion ne peut se produire que dans le domaine à commutation de paquets et que des mécanismes de QdS agissent en complémentarité avec l'application d'ingénierie de trafic pour les fins de QdS. De plus, en raison des erreurs de code dans OPNET et des incohérences soupçonnées dans le logiciel, des adaptations au code ont été réalisées.

Toutefois, les résultats obtenus sont globalement acceptables. L'évaluation de performance a illustré les contributions des protocoles adaptatifs aux composantes d'auto-similarité et de dépendance à long terme du trafic (particulièrement de TCP) ainsi que l'influence des tailles pour les tampons et les files d'attente. Elle a aussi révélé le rôle complémentaire et absolument nécessaire des autres mécanismes de contrôle de congestion. Les protocoles adaptatifs et les mécanismes de conditionnement doivent résister aux propriétés précitées du trafic en vue de combattre la congestion, à savoir celles d'auto-similarité et de dépendance à long terme du trafic.

Finalement, la solution mérite d'être considérée, car elle est tout à fait avant-gardiste par rapport à celles vues dans la littérature. En effet, elle définit le volet « disponibilité des ressources » et apporte des modifications au volet « politique ». Ainsi, elle enrichit à la fois le schéma de fonctionnement global et le mécanisme de contrôle d'admission qui est propre au domaine à commutation de paquets du réseau de cœur. Elle se présente aussi comme une solution ébauche qui offre un compromis tout autre entre l'utilisation des ressources et la qualité de service. Elle peut donc être raffinée et améliorée au fur et à mesure.

ABSTRACT

The UMTS authority of standardization (3GPP) is currently developing a management approach that uses service-based local policies. This solution relies upon the IP multimedia subsystem IMS and rests on a policy-based admission control. But, gaps can be found within the generic framework of 3GPP for the management approach, more precisely in their inherent aspects of « policy » and « resources availability ». This work formulates proposals for the approach and the application of interest. Both apply to the packet-switched domain of the UMTS core network.

Starting from the fifth UMTS release of standardization, a policy-based management approach is exerted in order to facilitate the system requirements. It supports the efforts of the network elements contributing to the end-to-end offer of quality of service. This solution rests on the multi-media subsystem (IMS) that supplements the packet-switched domain of the UMTS core network. But, if the efforts devoted to the definition of this approach are enormous within the generic framework of 3GPP, the aspects of « policy » and « resources availability » are prone to improvements. As for the first aspect, we can note the limitations of the defined policies, the small number of policy clients and the exclusive use of this form of management for the multimedia applications.

With regard to the « resources availability » aspect, it is almost not treated in 3GPP so that the form of management is, according to us, cut down by a fundamental component to its operation. This is rather surprising because it is well known that the traffic of third generation exhibits self-similarity and long-range dependence. These properties result in fluctuations in the traffic that are not only large in amplitude but also persistent over many time scales. They are ascribable with the various behaviours of the users and the unstable character of the adaptive protocols or the applications themselves. Thus, follow the inadequacy of the Markovian models, the invalidation of the associated results (queueing theory, estimates for the delay, loss and flow rate), the popularization of the distributions with heavy tail, etc. The studies thus recommend the measurement-

based admission control mechanisms for they are able to mitigate the incongruities of the traffic and the changes in the UMTS networks.

Consequently, we propose a diagram of operation and an admission control mechanism. Both are based on policies and measurements. The characteristics of the global solution are drawn from the literature and the generic frameworks of IETF and 3GPP. The modifications include the definition of new policies and the betterment of the 3GPP management diagram with the knowledge of the resources availability. The proposal uses pseudo-static L-LSP, a SGSN sheltering a policy client, a Bandwidth Broker lodging a SNMP manager, a policy server and the measurement-based admission control mechanism AC-MVEv2/AC-KQv2 and, finally, SNMP entities in the GSN nodes which proceed to the collection of the LSP utilization measurements. Moreover, the *Enhanced IP Subsystem Services* EISS replaces the *IP Multimedia Subsystem* IMS. It takes care of the contracts of high quality of service (multimedia applications, users, etc). All this results in the modification of the session establishment process for the sophisticated applications as well as in the addition of functionalities to some network elements.

In order to attest the quality of our solution, several experiments were carried out on OPNET version 10.5. The proof of concept related only to the aspect of « resources availability ». Moreover, only the algorithm AC-MVEv2 was considered. The adaptations to the simulation environment included the use of a non-UMTS network supporting MPLS and DiffServ as well as the usage of permissive QoS profiles, large sizes for the buffers and the queues, moderate levels of congestion and, finally, rather soft conditioning mechanisms. The goals were to identify the compromise of our solution in terms of QoS and resource consumption and to compare it with that of the OPNET solution, the latter being similar to the 3GPP proposition on this aspect because of its low content in QoS mechanisms. In this work, it is implied that the congestion can only occur in the packet-switched domain of the core network and that other QoS mechanisms act complementarily with the traffic engineering application for the

the purposes of QoS. In addition, because of the code errors in OPNET and the inconsistencies suspected in the software, adaptations to the code were also realized.

However, the results obtained are globally acceptable. The evaluation of performance illustrated the contributions of the adaptive protocols to the components in the traffic of self-similarity and long-range dependence (particularly of TCP). It also showed the influence of the sizes for the buffers and the queues. It moreover revealed the complementary and absolutely necessary role of the other congestion control mechanisms. The adaptive protocols and the conditioning mechanisms must resist the aforementioned properties of the traffic in order to fight the congestion - those of self-similarity and long-range dependence.

Finally, the solution deserves to be considered, because it is truly different from the ones found in the literature. Indeed, it defines the aspect « resources availability » and makes modifications to the one of « policy ». Thus, it enriches both the diagram of operation and the admission control mechanism of the packet-switched domain of the UMTS core network. It is also a draft solution that offers a new compromise between resources utilization and quality of service. Besides, it can be refined and progressively improved.

TABLES DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ABRÉVIATIONS

2G	Deuxième génération
3G	Troisième génération
3GPP	Third Generation Partnership Project
ACK	Acknowledgement
AC-MVE	Admission Control based on Mean Variance
AC-KQ	Admission Control based on Traffic Envelope
AF	Assured Forwarding
APN	Access Point Name
AS	Application Server
ATM	Asynchronous Transfer Mode
BB	Bandwidth Broker
BER	Bit Error Rate
BGCF	Breakout Gateway Control Function
BS	Bearer Service
BSC	Base Station Controller
BTS	Base Transceiver Station
CE	Certainty Equivalence
COPS	Common Open Policy Service
COPS-PR	COPS Usage for Policy Provisioning
CS	Circuit-Switched
CSCF	Call Session Control Function
CWTS	China Wireless Telecommunication Standard Group
DEC	COPS DECision message
DECT	Digital Enhanced Cordless Telecommunications
DiffServ	Differentiated Services

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRQ	COPS Delete ReQuest state message
DSCP	DiffServ CodePoint
EF	Expedited Forwarding
EPD	Encoded Provisioning Instance Data
ETSI	European Telecommunications Standards Institute
FEC	Forwarding Equivalence Class
FTN	FEC-to-NHLFE
FTP	File Tranfer Protocol
GCID	GPRS Charging IDentifier
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Telecommunications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
ICID	IM CN Subsystem Charging IDentifier
I-CSCF	Interrogating Call State Control Function
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identifier
IMT-DS	International Mobile Telecommunications Direct Spread
IMT-FT	International Mobile Telecommunications Frequency Time
IMT-MC	International Mobile Telecommunications Multi-carrier

IMT-SC	International Mobile Telecommunications Single carrier
IMT-TC	International Mobile Telecommunications Time Code
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
IntServ	Integrated Servies
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LPDP	Local Policy Decision Point
LRD	Long Range Dependance
MBAC	Measurement-Based Admission Control
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MIB	Management Information Base
MPEG	Moving Pictures Expert Group
MRF	Multimedia Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MPLS	Multi-Protocol Label Switching
MSC	Mobile Switching Center
MT	Mobile Terminaison
NHLFE	Next Hop Label Forwarding Entry
NRT	Non Real Time
OSA	Open Services Architecture
PBAC	Parameter-Based Admission Control
PBN	Policy-Based Networking
P-CSCF	Proxy Call State/Service Control Function
PCF	Policy Control Function

PDP	Policy Decision Point
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PHB	Per Hop Behaviour
PIB	Policy Information Base
PLMN	Public Land Mobile Network
PPRID	Prefix PRID
PRC	Provisioning Class
PRI	Provisioning Instance
PRID	Provisioning Instance Identifier
PS	Packet-Switched
PSTN	Public Switched Telephone Network
P-T	Policy-Target
P-TO	Policy Threshold
QdS	Qualité de Service
QoS	Quality of Service
QoS IE	QoS Information Element
RAB	Radio Access Bearer
RAP	Resource Allocation Protocol
RAN	Radio Link Control
REQ	COPS REQuest message
RFC	Request for Comments
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RPT	COPS RePorT state message
RSVP	Resource ReserVation Protocol
RT	Real Time
RTC	Réseau Téléphonique Commuté

RTO	Retransmission Timeout
RTT	Round Trip Time
SBLP	Service-based Local Policy
S-CSCF	Serving Call State Control Function
SDP	Session Description Protocol
SDU	Service Data Unit
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscription Locator Function
SNMP	Simple Network Management Protocol
SSF	Service Switching Function
SS7	Signalling System 7
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TD/SCDMA	Time Division Synchronous Code Division Multiple Access
TE	Terminal Equipement
TFT	Traffic flow Template
TLS	Transport Layer Security
T-SGW	Transport Signaling Gateway Function
TSPEC	Traffic Specification
UDP	User Datagram Protocol
UE	User Equipment
UIT	Union Internationale des Télécommunications
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
USIM	UMTS SIM
UTRA/FDD	Universal Terrestrial Radio Access Frequency Division Duplex

UTRA/TDD	Universal Terrestrial Radio Access Time Division Duplex
UTRAN	UMTS Radio Access Network
UWC	Universal Wireless Communications
UWC-136	Universal Wireless Communications
VBR	Variable Bit Rate
VoD	Video On Demand
VLR	Visitor Location Register
WCDMA	Wideband Code Division Multiple Access

SYMBOLES

Cx	Point de référence entre un CSCF et le HSS.
Dx	Point de référence entre le I-CSCF et le SLF.
Gi	Point de référence entre un réseau GPRS et un réseau à commutation de paquets externe
Gm	Point de référence entre un UE et le P-CSCF.
ISC	Point de référence entre un CSCF et un Application Server.
Iu	Point de référence entre un RNS et réseau cœur. Aussi considéré comme un point de référence
Le	Point de référence entre AS et GMLC
Mb	Point de référence vers services réseau IPv6
Mg	Point de référence entre MGCF et CSCF.
Mi	Point de référence entre CSCF et BGCF.
Mj	Point de référence entre BGCF et MGCF.
Mk	Point de référence entre deux BGCF
Mm	Point de référence entre CSCF et un réseau multimédia IP
Mr	Point de référence entre CSCF et MRFC.
Mw	Point de référence entre deux CSCF
Sh	Point de référence entre AS (SIP-AS ou OSA-CSCF) et HSS.
Si	Point de référence entre IM-SSF et HSS.

LISTE DES ANNEXES

CHAPITRE 1
INTRODUCTION

La complexification des réseaux UMTS est en partie le contrecoup des efforts de convergence déployés par les groupes de standardisation avec l'Internet. À la cinquième version de normalisation de ces systèmes, un domaine unique à commutation de paquets est censé véhiculer l'ensemble des applications : voix, multimédias, et autres. Ainsi, de version en version, le groupe 3GPP raffine ses solutions de contrôle de congestion afin de mieux composer avec les contraintes antinomiques reliées à l'utilisation des ressources et à la qualité de service. En vue de faciliter la configuration conséquente des réseaux pour diverses fins, une approche de gestion fondée sur les politiques des services a été adoptée ainsi qu'un mécanisme de contrôle d'admission basé sur des politiques. Cette application d'ingénierie de trafic repose sur les politiques de l'opérateur et sur les ressources disponibles dans le réseau. Ce mémoire étudie ces solutions et se concentre sur le domaine à commutation de paquets du réseau cœur d'UMTS. Il traite de leurs volets « politique » et « disponibilité des ressources » et formule des propositions susceptibles de les améliorer. Dans ce chapitre d'introduction, des concepts de base sont d'abord énoncés relativement aux réseaux UMTS. Ensuite, sont exposés les éléments de la problématique, puis les objectifs de recherche, et, enfin, le plan du mémoire.

1.1 Définitions et concepts de base

Les réseaux UMTS s'inscrivent à l'intérieur de la famille disparate IMT-2000, une mosaïque de normes régionales promue par l'*Union Internationale des Télécommunications*. L'élaboration des spécifications d'UMTS revient au projet de partenariat 3GPP regroupant plusieurs acteurs de standardisation.

1.1.1 Normalisation d'UMTS

Les réseaux mobiles UMTS s'octroient le titre de membre IMT-2000 en apportant une couverture plus large, des services plus variés ainsi que des débits et une capacité en nombre d'abonnés supérieurs. Ils trouvent leurs prédécesseurs chez les systèmes GSM-GPRS.

D'abord, la mobilité universelle s'accomplit à l'aide d'une structure hiérarchisée qui intègre des composantes satellites et terrestres [1]. Avec ses deux modes d'accès radio, l'UTRAN permet d'assurer la couverture au niveau terrestre suivant des macro, micro et picocellules. En effet, UTRA FDD, l'un des deux modes, convient aux trafics symétriques et aux environnements intérieurs avec mobilité restreinte. Le mode UTRA TDD, quant à lui, est plutôt adapté aux trafics asymétriques et aux environnements extérieurs avec grande mobilité.

Ensuite, quatre classes de qualité de service ont été définies pour les applications UMTS [1, 2]. Les deux premières englobent les applications en temps réel, aux contraintes de délai assez importantes. Les deux autres, généralement utilisées pour transporter les applications Internet traditionnelles, sont plus tolérantes au délai et peuvent donc fournir des taux d'erreur moindres en faisant usage des techniques de codage de canal et de retransmission. Les tolérances au délai dictent les priorités devant être attribuées à ces classes pour des fins diverses, notamment pour l'ordonnancement. Le Tableau 1.1 présente succinctement ces classes de trafic, lesquelles se distinguent, essentiellement, en fonction de leur tolérance au délai.

Enfin, les débits envisagés permettent de desservir trois catégories d'usagers mobiles : un débit de 144 kbps est fourni aux usagers ruraux de mobilité élevée (extérieur rural et vitesse maximale de 300 km/h); un débit de 384 kbps est attribué aux usagers urbains de mobilité moyenne (extérieur urbain et vitesse inférieure à 50 km/h) et, enfin, un débit limite de 2 Mbps est accordé aux usagers de mobilité réduite se trouvant à l'intérieur [1].

Tableau 1.1 Classes de qualité de service UMTS

	Classe de trafic et description	*Délai*	*Débit (kbps)*	*Tolérance aux erreurs*	*Exemples*
Temps réel	**Conversationnelle** - relation (variation) temporelle conservée entre entités de flot - patron de type conversationnel et contrainte dure sur le délai	**<< 1 s**	32 - 384 kbps	Oui	- téléphonie - visiophonie
			1 kbps	Non	- jeux interactifs
	À flux continu - relation (variation) temporelle conservée entre entités de flot	**≈ 1 s**	32 - 128 kbps	Oui	- audio haute qualité
			Non garanti	Non	- images fixes
	Interactive - patron type requêtes-réponses - contenu préservé	**< 1 s**	Non garanti	Non	- commerce électronique
			Non garanti	Non	- navigation sur Internet
	Arrière-plan - contenu préservé - la destination n'attend pas la réponse à l'intérieur d'un temps donné, donc pas de contrainte réelle pour le délai	**> 10 s**	Non garanti	Oui	- fax
			Non garanti	Non	- messagerie électronique avec acquittement

À titre indicatif, le cadre générique de 3GPP comporte les documents des versions de normalisation d'UMTS (voir Annexe A.2). Notre étude porte sur la version 5, car elle pose des jalons véritables vers le tout-IP.

1.1.2 Composantes du réseau UMTS

L'architecture de référence illustre successivement l'usager, l'infrastructure radio, puis le réseau cœur qui est connecté à un réseau dorsal. L'usager UE ou *User Equipment* est constitué du module d'identité « universel » des services de l'abonné USIM ainsi que de l'équipement mobile (ME), lequel est à son tour composé d'un équipement terminal (*Terminal Equipment* TE) et d'une terminaison mobile (*Mobile Terminaison* MT) [1, 2, 4].

Sous-réseau radio de l'architecture de référence

En amont du réseau cœur, on trouve le point névralgique du système UMTS, l'interface radio UTRAN *UMTS Radio Access Network*. Elle inclut des NodeB et des RNC, les équivalents des stations de base BTS et des contrôleurs de stations de base BSC du GSM. Parmi les éléments qui distinguent l'UTRAN de l'interface radio du GSM, citons ses technologies UTRA fondées sur W-CDMA, ses quatre nouvelles interfaces (Uu, Iu, Iur, Iub), sa capacité à gérer la macrodiversité et les relèves « soft » et son utilisation d'ATM dans la couche de transport. Les réseaux tout-IP emploieront DiffServ et MPLS. Les interfaces Uu et Iu regroupent, respectivement, les protocoles qui permettent d'acheminer le trafic depuis l'usager jusqu'à l'UTRAN et depuis celui-ci jusqu'au réseau cœur. L'interface Iub relie un RNC à un NodeB et l'interface Iur sépare deux RNC. Par ailleurs, ce sous-réseau exécute une série de fonctions, notamment le transfert des données, le chiffrement/déchiffrement des données, la gestion de la micro-mobilité et la gestion des ressources radio avec le contrôle d'admission, l'allocation/désallocation des ressources et le contrôle de puissance.

Sous-réseau cœur de l'architecture de référence

Le réseau cœur prend ensuite la relève, avec ses domaines à commutation de circuits et de paquets (*Circuit-Switched CS* et *Packet-Switched* PS). Relié à l'UTRAN par l'interface Iu-CS, le premier domaine comprend essentiellement des MSC/VLR. Ce domaine dédié à l'acheminement des applications de voix est absent des réseaux tout-IP. Connecté au réseau radio par l'interface Iu-PS, le second domaine permet de convoyer les trafics rattachés aux services à commutation de paquets. Parmi les éléments architecturaux de celui-ci, on trouve le nœud de service GPRS ou SGSN (*Serving GPRS Support Node*) et le nœud passerelle du GPRS ou GGSN (*Gateway GPRS Support Node*). Le SGSN achemine les paquets depuis l'UTRAN jusqu'à la zone qu'il dessert et se charge des procédures liées au routage, à la gestion de la mobilité intra-SGSN et à l'authentification. Le GGSN fait le pont entre le réseau fédérateur GPRS et les réseaux à commutation de paquets externes (Internet, etc.) via l'interface Gi. Il gère la macro-

mobilité et peut procéder à une gestion basée sur des politiques. Ce domaine PS effectue aussi la tarification et l'allocation des ressources du réseau cœur. Il emploie DiffServ et MPLS pour la QdS.

Sous-système multimédia IMS ou IP Multimedia Subsystem (version 5)

Dans la perspective de véhiculer sur un domaine unique à commutation de paquets le trafic des applications et services sophistiqués, le sous-système multimédia IMS a été greffé à l'architecture initiale d'UMTS à la version 5 de normalisation. La Figure 1.1 détaille la nouvelle architecture pour le domaine susnommé et le sous-système multimédia IMS [1, 2, 4, 5].

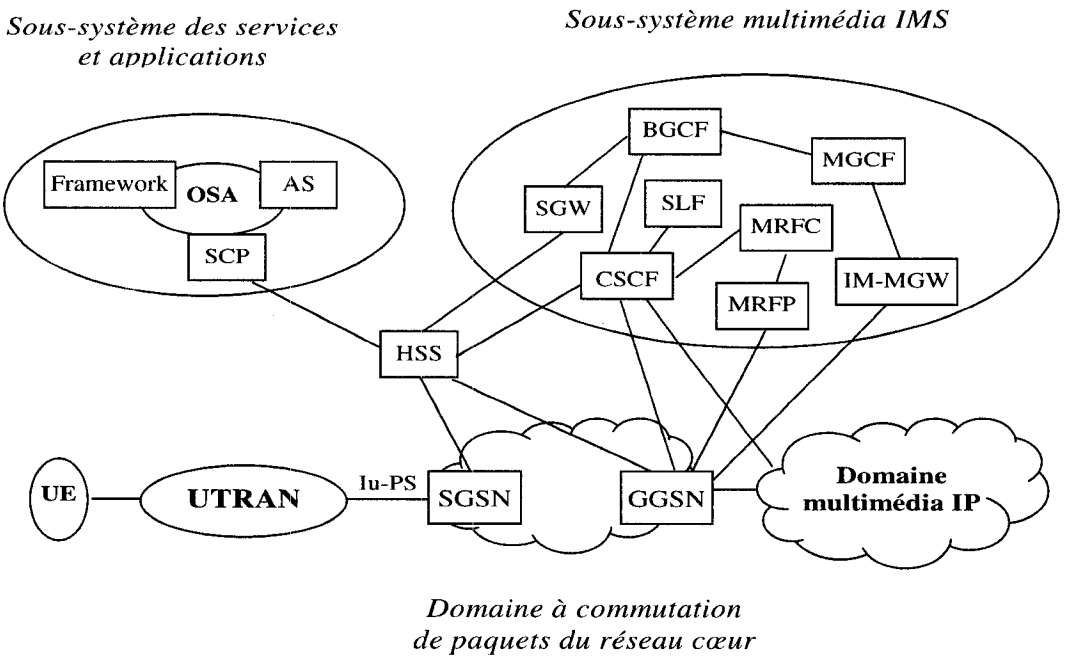

Figure 1.1 Architecture globale d'UMTS de la version 5

En plus de supporter les applications multimédias, le nouveau domaine convoie le trafic des applications traditionnelles de voix. Il est donc connecté au réseau IP multimédia externe et, si le domaine à commutation de circuits est absent, au réseau RTC qui est relié à IMS. Ce module de la version 5 permet de converger vers le « tout-IP ». Il est détaillé au chapitre deux.

1.2 Éléments de la problématique

Dans UMTS, la gestion fondée sur des politiques est pilotée par le sous-système multimédia IMS, une extension au domaine à commutation de paquets du réseau de cœur. Cette approche de gestion et le contrôle d'admission basé sur des politiques, son application fille, reposent sur les ressources disponibles et sur les politiques de l'opérateur. Ci-après, nous décrivons les éléments de la problématique qui sont rattachés à leurs volets inhérents « politique » et « disponibilité des ressources ».

En ce qui concerne le volet « politique », il faut souligner que le système UMTS est en phase de normalisation. L'IETF a développé l'approche de gestion, de même que l'application, afin de faciliter la configuration des réseaux et, ce, dans le but de servir les intérêts d'une variété de domaines [2, 4, 5, 8, 9, 10]. Entre autres choses, l'adoption de ces solutions permet de remédier à l'hétérogénéité des spécifications de QdS des opérateurs. Cependant, dans 3GPP, les politiques circonscrivant la solution de gestion sont peu variées, car elles sont associées aux applications multimédias et exclusivement liées aux services. De plus, la passerelle GGSN est l'unique nœud tenu d'incorporer un client de politiques, car l'usager n'est pas obligé d'abriter un client de politiques et les autres nœuds sont ignorants de politiques. Ainsi, l'approche de gestion de 3GPP peut sembler disposer d'un degré d'automatisme inférieur à celui envisagé par l'IETF.

Quant au volet « disponibilité des ressources », il est peu traité dans 3GPP. Toutefois, les méthodes de surdimensionnement et de conditionnement (MPLS, DiffServ) sont préconisées pour le domaine. De plus, il appert que le mécanisme de contrôle d'admission et d'aptitude du SGSN est classique, car il émet des décisions en se basant uniquement sur la disponibilité des ressources, par opposition à celui du GGSN. Dans tous les cas, ce volet est spécifique à l'opérateur ou au vendeur. Pourtant, le trafic présente des fluctuations grandes en amplitude et persistantes sur plusieurs échelles de temps, ce qui lui confère les propriétés excentriques de dépendance à long terme et d'auto-similarité [15 - 23]. En conséquence, les modèles markoviens et les résultats qui en découlent ne conviennent plus. Cela dit, les mécanismes de contrôle d'admission basés sur des mesures sont recommandés par les études. Mais, la performance de ces

mécanismes dépend d'une variété de facteurs, notamment des propriétés du trafic, des conditions dans le réseau et des processus pour l'acquisition des mesures et l'analyse.

À la lumière de ces constatations, nous formulons des propositions susceptibles de concourir à la continuité de la QdS. La solution composite est obtenue après examen des spécifications des instances 3GPP et IETF et des recommandations de la littérature.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir un mécanisme de contrôle d'admission basé sur des politiques pour le domaine à commutation de paquets du réseau cœur d'UMTS. Nous définissons les objectifs spécifiques suivants :

- analyser les solutions existantes pour les volets « politique » et « disponibilité des ressources » en procédant à un examen du schéma de gestion de 3GPP et à une revue des mécanismes actuels de contrôle d'admission ;
- concevoir à la fois un contrôle d'admission et un schéma de fonctionnement qui reposent sur des politiques et des mesures pour le domaine à commutation de paquets ;
- implémenter et évaluer la performance du schéma de fonctionnement et du mécanisme de contrôle d'admission afin d'attester de leur efficacité.

1.4 Plan du mémoire

Le corps du mémoire est construit sur cinq chapitres. Le deuxième suit l'introduction et présente la revue de littérature d'intérêt. Le troisième propose un schéma de fonctionnement basé sur des politiques ainsi qu'un algorithme de contrôle d'admission basé sur des politiques et des mesures pour le domaine à commutation de paquets du réseau cœur d'UMTS. Le quatrième chapitre détaille l'implémentation et les résultats de l'évaluation de performance. Le cinquième conclut ce mémoire.

CHAPITRE 2
GESTION BASÉE SUR DES POLITIQUES ET MÉCANISMES DE CONTRÔLE D'ADMISSION

Le concept de qualité de service dans les réseaux recouvre les notions individuelles de largeur de bande, de délai, de gigue, de taux de perte et de disponibilité. Il revêt une importance considérable dans le cadre des réseaux UMTS, car ceux-ci sont liés à des entités externes de façon ferme par des contrats de QdS. Ces réseaux doivent intégrer des mécanismes robustes en vue de satisfaire autant que possible la contrainte lourde de continuité de la qualité de service. Ce mémoire est dédié à la gestion basée sur des politiques dans les réseaux UMTS et, particulièrement, au mécanisme de contrôle d'admission basé sur des politiques qui en résulte. Ce chapitre examine les solutions de gestion basée sur des politiques et celles susceptibles de l'enrichir, c'est-à-dire qu'il explore les solutions reliées aux volets « disponibilité des ressources » et « politique » de ce mémoire. D'entrée de jeu, les concepts de base de QdS UMTS sont énoncés. Ensuite, le sous-système multimédia IMS est présenté et un avant-goût du cadre générique de 3GPP sur le sujet d'intérêt est donné. Après ce préambule, sont explorés le cadre générique de l'IETF associé au protocole COPS, puis celui de l'IETF lié au modèle dérivé COPS-PR et, enfin, le cadre générique de 3GPP. Par la suite, nous traitons des solutions qui se rapportent au « volet disponibilité des ressources » du mémoire, c'est-à-dire des mécanismes de contrôle d'admission basés sur des mesures. Le chapitre se termine enfin sur une liste non exhaustive de problèmes ouverts.

2.1 Concepts de base liés à la qualité de service UMTS

Il ressort que la qualité de service UMTS fait intervenir des notions nouvelles, notamment celle de contexte PDP qui est fondamentale à la compréhension des chapitres subséquents. Cette section explique ce concept, l'architecture UMTS et ses fonctions de gestion de QdS.

2.1.1 Contexte PDP

Dans le domaine à commutation de paquets d'UMTS, un trafic donné emprunte un tunnel préalablement établi entre la source et la destination pour la durée de la session. Ce tunnel, que l'on dénomme contexte PDP, est créé lors de la procédure spécifique d'activation de contexte qui met en branle, dans les différents sous-réseaux, plusieurs processus de contrôle [1, 2]. C'est après s'être attaché au réseau que l'usager en fait la demande – le réseau peut aussi l'initier. Les caractéristiques de la session sont alors négociées entre les parties impliquées. À l'issue du dialogue doivent être arrêtés le type du protocole qui sera utilisé (ex. Ipv4), l'adresse PDP du terminal mobile (IP), la qualité du service de support à mettre en place ainsi que l'adresse du GGSN qui sert de point d'accès au réseau à commutation de paquets externe (APN *Access Point Name*). L'adresse PDP du mobile permettra aux réseaux externes de le visualiser. De plus, les valeurs des attributs de QdS du support sont choisies en fonction des exigences des applications à transporter (ex. : service interactif). Elles sont négociées au départ, mais peuvent être modifiées dynamiquement avec la procédure de modification de contexte. Le contexte PDP est conservé dans le terminal mobile, le SGSN et la passerelle GGSN.

2.1.2 Architecture globale de qualité de service UMTS

Au terme de la procédure d'activation de contexte PDP seront activés les différents « services de support » qui concourent à la continuité de la qualité de service souhaitée. Celle-ci est obtenue à l'aide d'une architecture modulaire à plusieurs niveaux où les services d'une couche donnée s'appuient sur ceux de la couche inférieure pour exercer ses fonctions. La Figure 2.1 illustre les strates qui définissent l'architecture de QdS UMTS permettant de respecter le contrat de QdS des applications [1, 2, 4]. Les blocs verticaux représentent l'équipement terminal de l'usager (TE), sa terminaison mobile (MT), le réseau radio (UTRAN), le nœud SGSN du réseau cœur, la passerelle du réseau cœur (GGSN) et, enfin, l'équipement terminal de l'usager de destination. L'Annexe A.3 indique les valeurs possibles des attributs de QdS du service de support UMTS. Celles du réseau cœur relèvent du choix de l'opérateur.

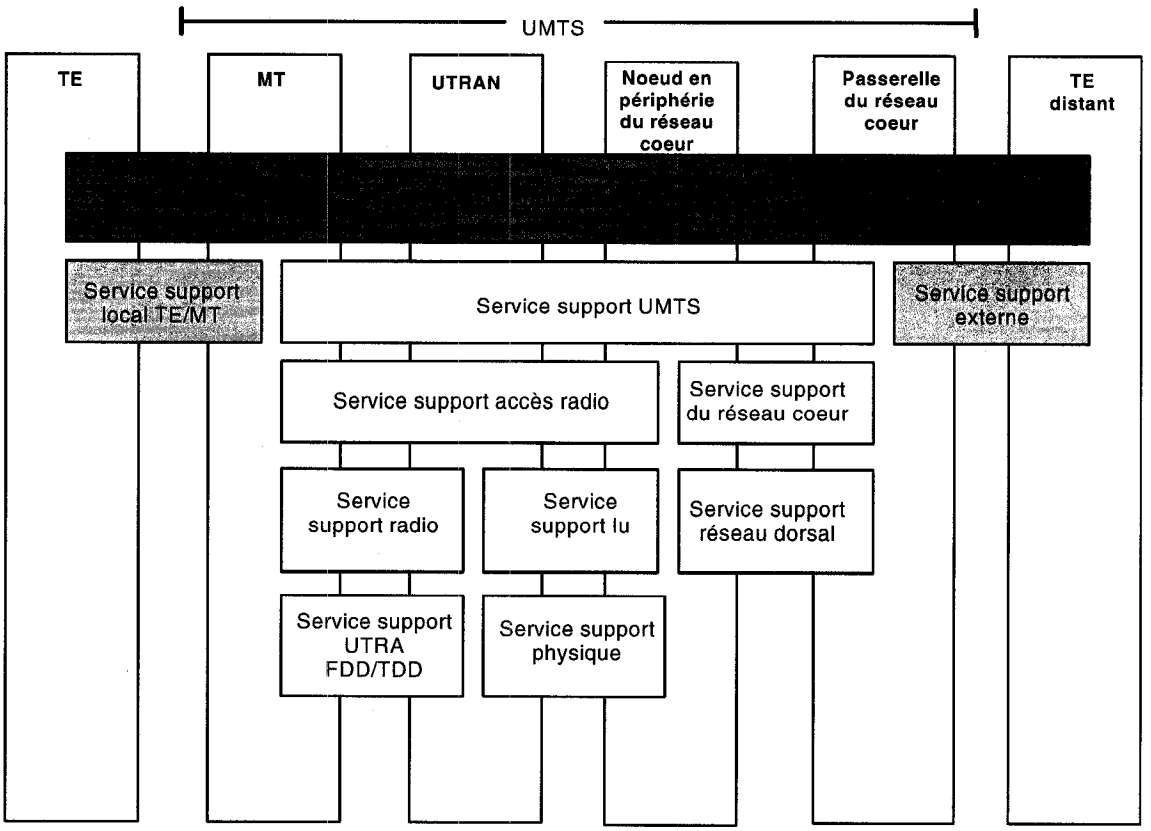

Figure 2.1 Architecture de qualité de service UMTS

2.1.3 Fonctions de gestion de QdS de la couche UMTS

Pour réaliser l'établissement, la modification et la maintenance des services de support, une série de modules de gestion de QdS sont placés sur la couche UMTS. Cette section présente les fonctions de gestion qui s'inscrivent dans les plans de contrôle et de transmission de l'architecture de QdS d'UMTS.

Fonctions de gestion de QdS sur le plan de contrôle de la couche UMTS

Dans le plan de contrôle, on trouve les modules de traduction, de contrôle d'admission/aptitude et les gestionnaires de services de support (local, UMTS, d'accès radio, etc.) [1, 2, 4]. Les opérations effectuées sur ces véhicules de trafic se traduisent à

la fois par des procédures de signalisation/négociation qui font intervenir les services externes et par l'établissement/ modification des services sous-jacents.

Dans tous les nœuds figure un module *gestionnaire de service de support* qui s'acquitte de coordonner les modules pour la mise en place, la modification et la maintenance des services de support. Il fournit les attributs pertinents aux fonctions de gestion du plan usager, utilise les services d'autres instances ou offre les siens, communique avec les autres gestionnaires et interroge des modules pour voir s'il est autorisé à répondre favorablement à une requête. Il convertit aussi, au besoin, ses attributs en ceux du service de support qui est situé sur la couche inférieure et qui doit lui fournir du soutien. De plus, la *fonction de traduction* est installée dans les nœuds périphériques pour des raisons évidentes. Les gestionnaires de l'usager et de la passerelle GGSN utilisent ce module chargé de la conversion des primitives internes d'UMTS en signalisation externe et de la mise en correspondance des attributs de service. Entre autres, les attributs d'UMTS peuvent être mis en correspondance avec le TSPEC de l'IETF ou avec les paramètres du service local. Les gestionnaires déterminent les attributs des services de support dont ils veulent solliciter l'aide dans l'exercice de leurs fonctions. C'est le cas, par exemple, de celui du GGSN qui l'utilise pour identifier les attributs des éléments accès radio, Iu et réseau cœur, et qui demande à leurs gestionnaires attitrés de s'exécuter après leur avoir transmis ces informations. Dans ces nœuds, on trouve aussi un module de *contrôle d'admission/aptitude*. Il connaît les ressources consommées et celles allouées aux services de support UMTS. Il vérifie la disponibilité des ressources au niveau de l'entité avant d'admettre une requête d'activation/modification de contexte, puis les réserve si elles sont allouées au service de support UMTS. De plus, il s'assure que le nœud peut offrir le service, c'est-à-dire qu'il vérifie si le service est implémenté et activé. Les gestionnaires interrogent leur module d'admission/aptitude. Enfin, le module de *souscription* vérifie si l'usager est autorisé à utiliser le service en examinant les attributs de QdS de l'usager et ses droits administratifs dans le HSS. Le gestionnaire du GGSN interroge ce module à cette fin.

Les fonctions de gestion de QdS UMTS sur le plan de contrôle sont montrées à la Figure 2.2.

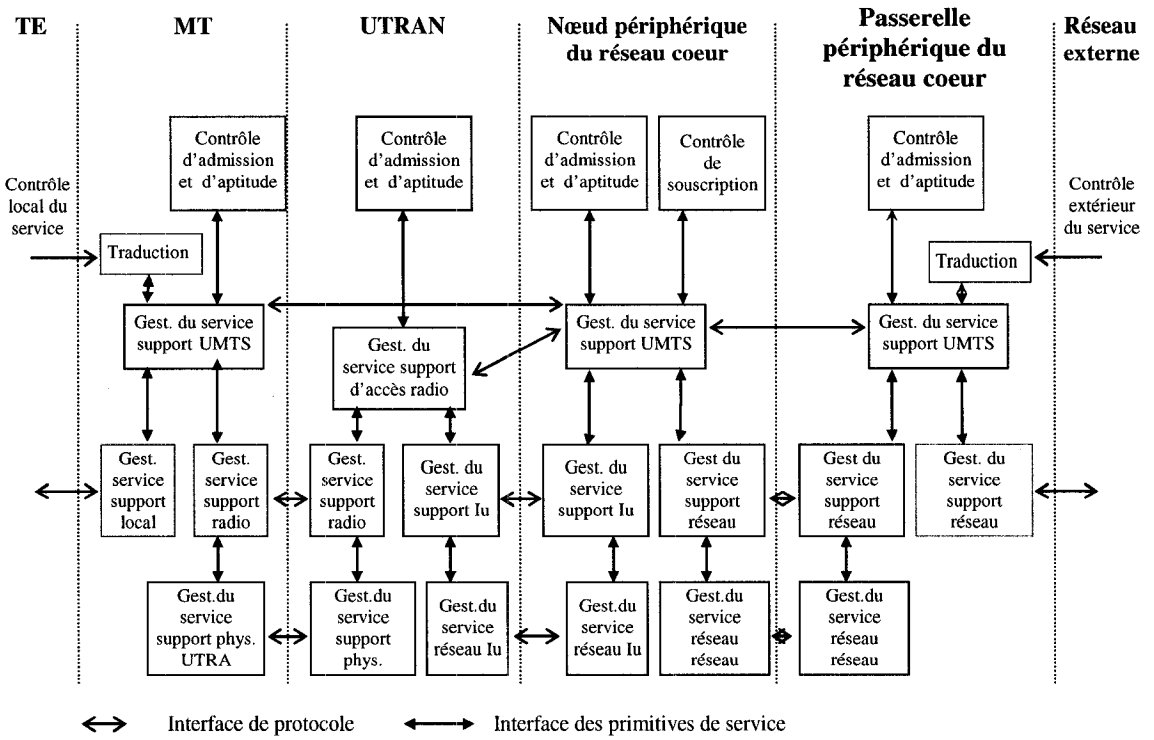

Figure 2.2 Fonctions de gestion de QdS sur le plan de contrôle UMTS

Fonctions de gestion de QdS sur le plan de transmission de la couche UMTS

Il incombe aux modules de gestion de QdS du plan usager de tout mettre en œuvre afin de respecter le contrat de QdS qui est établi pour le service de support UMTS [1, 2, 4]. Ils veulent borner les trafics de signalisation et de données usager. L'entente est conclue à l'issue des négociations entre les modules de contrôle.

Dans l'UTRAN et les nœuds GSN, on trouve la *fonction de mise en correspondance*. Celle-ci pose une étiquette sur chaque unité de donnée afin de dicter aux éléments du réseau la QdS qu'ils doivent respecter. La *fonction de classification*, quant à elle, est utile à la terminaison mobile MT et au GGSN. Elle assigne à un service de support UMTS les unités qui proviennent des services de support externe et local et,

ce, en fonction des attributs de QdS qu'elle extrait de l'en-tête ou des caractéristiques des unités. En ce qui a trait au *gestionnaire de ressources*, il réside dans la terminaison mobile, l'UTRAN, le SGSN et le GGSN. Il répartit les ressources disponibles entre les services concurrentiels en se basant sur les attributs de QdS signalés. Il peut prendre des formes diverses, notamment celle d'un module d'ordonnancement ou encore d'une fonction de contrôle de puissance radio. Enfin, la terminaison mobile de l'usager, l'UTRAN et le GGSN hébergent le module de *conditionnement de trafic*. Cette fonction assure la conformité entre l'unité de trafic et la qualité de service négociée pour le service. Les techniques employées sont la mise en forme (*shaping*) et l'inspection (*policing*). La première méthode modèle l'unité de trafic en se basant sur le contrat de QdS (par ex., seau à jetons). La seconde examine les attributs de QdS de l'unité et, si nécessaire, la rejette ou lui pose une étiquette de non conformité en cas de congestion. Les fonctions de gestion sur le plan de transmission sont illustrées à l'Annexe A.4.

L'architecture d'UMTS est modifiée à la version 5 de 3GPP pour intégrer, en plus des modules précités, des fonctions de gestion de QdS pour le moins sophistiquées. Celles-ci appartiennent au sous-système multimédia IMS.

2.2 Sous-système multimédia IMS

À la version 5 de 3GPP, le sous-système multimédia IMS (*IP Multimedia Subsystem*) est greffé à l'architecture de base d'UMTS dans le but de gérer les applications propres aux domaines IP multimédias [5]. Il se présente comme une extension au domaine PS, car ses trafics de signalisation et de données empruntent les services de support de ce domaine. Il abrite le serveur local des abonnés HSS (*Home Subscriber Server*), les serveurs SIP CSCF (*Call State/Service Control Function*) ainsi que les entités d'interfonctionnement dédiées au contrôle et à la conversion des données. Le HSS et les CSCF sont présentés.

Au cœur du réseau, on trouve le serveur local d'abonnés désigné par le terme *HSS*, un acronyme pour *Home Subscriber Server*. Ce module est un super-ensemble du HLR des réseaux GSM/GPRS. En effet, il renferme des informations additionnelles sur

les abonnés pour IMS et possède des interfaces avec le S-CSCF et le I-CSCF afin de leur acheminer les informations de souscription et de localisation de l'usager. Les quintuplets qu'il conserve sont utilisés pour l'authentification, la confidentialité et l'intégrité. Il détient la liste des serveurs renfermant les services et les applications, possède des interfaces avec ceux-ci, connaît les services et applications auxquels les abonnés ont souscrit et les offre. Il autorise les services, les applications et l'itinérance. Ensuite, les nœuds CSCF sont scindés en trois entités : le nœud de service S-CSCF, la fonction d'interrogation I-CSCF et le serveur mandataire P-CSCF.

En ce qui concerne la fonction *S-CSCF*, ou *Serving Call State Control Function*, elle contribue à la facturation, elle contrôle les sessions des usagers enregistrés et supporte les applications à l'aide des plates-formes de services. Elle accepte aussi les requêtes d'enregistrement de l'usager et les authentifie à l'aide des quintuplets du HSS. Lors de cette étape préalable à l'échange des données, le profil de l'usager dans le HSS est téléchargé dans le S-CSCF. Plusieurs serveurs S-CSCF peuvent cohabiter dans un même réseau afin d'augmenter sa capacité et ses fonctionnalités. En outre, le réseau d'origine peut abriter la *fonction d'interrogation I-CSCF ou Interrogating Call State Control Function*. Ce nœud facultatif pour IMS constitue le premier point de contact pour les messages de signalisation en provenance de l'extérieur. Il sélectionne un S-CSCF pour l'usager ayant formulé une requête d'enregistrement et le lui assigne après avoir procédé à une répartition de charge basée sur les données du HSS (*load balancing*). Il peut contribuer à la facturation et masquer de l'extérieur les informations relatives à la configuration, la topologie et la capacité du réseau.

Finalement, le dernier nœud CSCF est le serveur mandataire CSCF dénommé *P-CSCF* (*Proxy Call State Control Function*). Il constitue le premier point de contact à l'intérieur du sous-système multimédia IMS pour les usagers qui circulent dans leur réseau d'origine ou qui sont en itinérance. Il véhicule les messages entre le réseau et l'usager, convoie les requêtes d'enregistrement vers le I-CSCF et achemine les messages dédiés au serveur S-CSCF. En plus de sécuriser l'accès au mobile, il gère les appels

d'urgence locaux et compresse les messages. Il permet la gestion basée sur les politiques des services. L'Annexe A.5 fournit des détails sur IMS et ses procédures.

À titre indicatif, le sous-système multimédia est indépendant du type d'accès utilisé. Enfin, les modifications de la version 5 gravitent autour de trois points essentiels : l'emploi d'un protocole de l'IETF pour les sessions (SIP), l'utilisation d'un mécanisme de corrélation entre les couches session et GPRS, et l'ajout de modules de contrôle et de liaison avec des réseaux à commutation de paquets et de circuits.

2.3 Gestion de la qualité de service IP de bout-en-bout

En raison des applications IMS, les couches IP et UMTS hébergent, à partir de la version 5, des modules supplémentaires. La gestion des réseaux est désormais basée sur des politiques. Dans cette section, après avoir motivé l'emploi d'un mécanisme de corrélation entre les couches session et GPRS, nous décrivons les fonctions de gestion de QdS IP qui agissent de concert avec les modules de QdS d'UMTS susmentionnés.

2.3.1 Corrélation entre les couches session et GPRS

Dans 3GPP, la gestion basée sur des politiques dissimule, d'emblée, la notion de corrélation. Les paramètres de QdS requis pour une session multimédia IP sont découverts par le réseau au préalable, c'est-à-dire avant la réservation des ressources GPRS dans le domaine à commutation de paquets. De plus, le trafic de signalisation de la session emprunte un chemin différent de celui des données. Ce sont ces deux raisons qui justifient l'emploi d'un mécanisme de corrélation entre les couches session (SIP) et GPRS (*binding information*) [5, 11]. L'information de corrélation spécifie un (des) identificateur(s) de flot(s) IP et un jeton d'autorisation. Elle désigne donc sans équivoque une session autorisée. En fait, au début de l'établissement d'une session, les paramètres de QdS de l'application (SDP) sont transmis à un serveur de politiques situé dans IMS. Ensuite, à l'aide de ces informations, les politiques pertinentes sont indexées par ce dernier d'une centrale de dépôt. Un état d'autorisation est ensuite installé dans

celui-ci, puis un jeton est créé pour la session et envoyé à l'usager. L'information de corrélation doit être insérée dans les requêtes d'activation et de modification de contexte de l'usager qui sont associées à des applications multimédias et de voix sur IP. Elle est employée pour valider les requêtes auprès du serveur de politiques. Elle peut être précisée dans les messages RSVP pour associer les sessions RSVP et SIP.

2.3.2 Fonctions de gestion de la qualité de service à la couche IP

À partir de la version 5, la couche IP abrite donc des fonctions de gestion de QdS fondées sur des standards de l'IETF. Celles-ci permettent la gestion basée sur des politiques et sont impliquées dans le contrôle des services de support IP externes [5, 9, 10]. Cette section traite des fonctions de QdS IP qui sont hébergées chez l'usager, le GGSN et le sous-système multimédia IMS.

Fonctions de gestion de QdS de l'usager

L'usager peut supporter le mécanisme de corrélation (*binding mechanism*), incorporer une fonction de traduction/mise en correspondance et comporter un gestionnaire de service de support IP. L'information de corrélation permet au GGSN de renforcer les politiques basées sur des services (SBLP). Le gestionnaire peut contenir à son tour un point de renforcement de politiques PEP (*Policy Enforcement Point*) et intégrer des fonctions de QdS IP telles que DiffServ et RSVP/IntServ. La fonction de traduction interprète et met en correspondance les paramètres SDP de l'application avec les attributs du contexte PDP (ou, si un gestionnaire est présent, avec les attributs IP).

Fonctions de gestion de QdS de la passerelle du réseau coeur GGSN

Le GGSN peut supporter le mécanisme de corrélation, inclure une fonction de traduction/mise en correspondance et intégrer un gestionnaire de service de support IP. Le module de traduction fait la conversion IP-UMTS des attributs de QdS. Les paramètres DiffServ sont configurés à l'avance, dérivés du contexte PDP et/ou

déterminés à partir des attributs RSVP. Son gestionnaire doit abriter un PEP pour participer à la gestion basée sur des politiques. Si l'usager et le GGSN contiennent un gestionnaire, ils communiquent entre eux directement. Pour la gestion basée sur des politiques, le GGSN peut se baser sur les données RSVP et/ou DiffServ de l'usager ou traduire les paramètres du contexte PDP signalés entre les gestionnaires des services de support UMTS. Le SGSN peut toutefois privilégier les données du profil de souscription HSS. Le Tableau 2.1 montre les aptitudes des gestionnaires de ces nœuds.

Tableau 2.1 Aptitudes du gestionnaire dans les nœuds GGSN et usager

Aptitude	*Usager UE*	*Passerelle GGSN*
Fonction frontière DiffServ	Facultatif	Requis
RSVP/IntServ	Facultatif	Facultatif
Point de renforcement des politiques	Facultatif	Requis *

Par ailleurs, le GGSN exécute un contrôle d'admission basé sur des politiques et configure une porte d'accès *gate*. Le contrôle d'admission s'appuie, entre autres, sur les attributs autorisés par le PCF. La porte d'accès constitue la composante usager de la fonction PEP ; elle est envoyée par le PCF dans une décision d'autorisation de réservation des ressources. Elle discrimine les paquets à l'aide d'un classificateur et d'un état. Le classificateur agit sur un flot unidirectionnel grâce au quintuplet défini par les adresses IP source et destination, leurs ports et le protocole. L'état, fermé au départ, devient ouvert sur ordre du PCF et redevient fermé lorsque l'autorisation est enlevée. Sur la liaison descendante, les paquets sont soumis aux portes installées et, s'ils ne sont discriminés par aucune d'entre elles, ils sont examinés par les filtres TFT fournis par l'usager. Sur la liaison montante, s'ils sont reconnus par une porte et si celle-ci est ouverte, ils sont traités en fonction des actions prévues, sinon ils sont rejetés.

Fonctions de gestion de QdS du sous-système multimédia IMS

Le sous-système multimédia abrite le serveur P-CSCF décrit précédemment et la fonction *PCF* ou *Policy Control function*. Ces modules sont impliqués dans la gestion basée sur des politiques : le P-CSCF supporte le mécanisme de corrélation et la fonction PCF envoie des décisions de politiques au PEP du GGSN (interface Go). Ils peuvent être co-localisés; toutefois, s'ils sont séparés, leur interface n'est pas définie dans les documents de la version 5. La Figure 2.5 montre les fonctions de QdS IP.

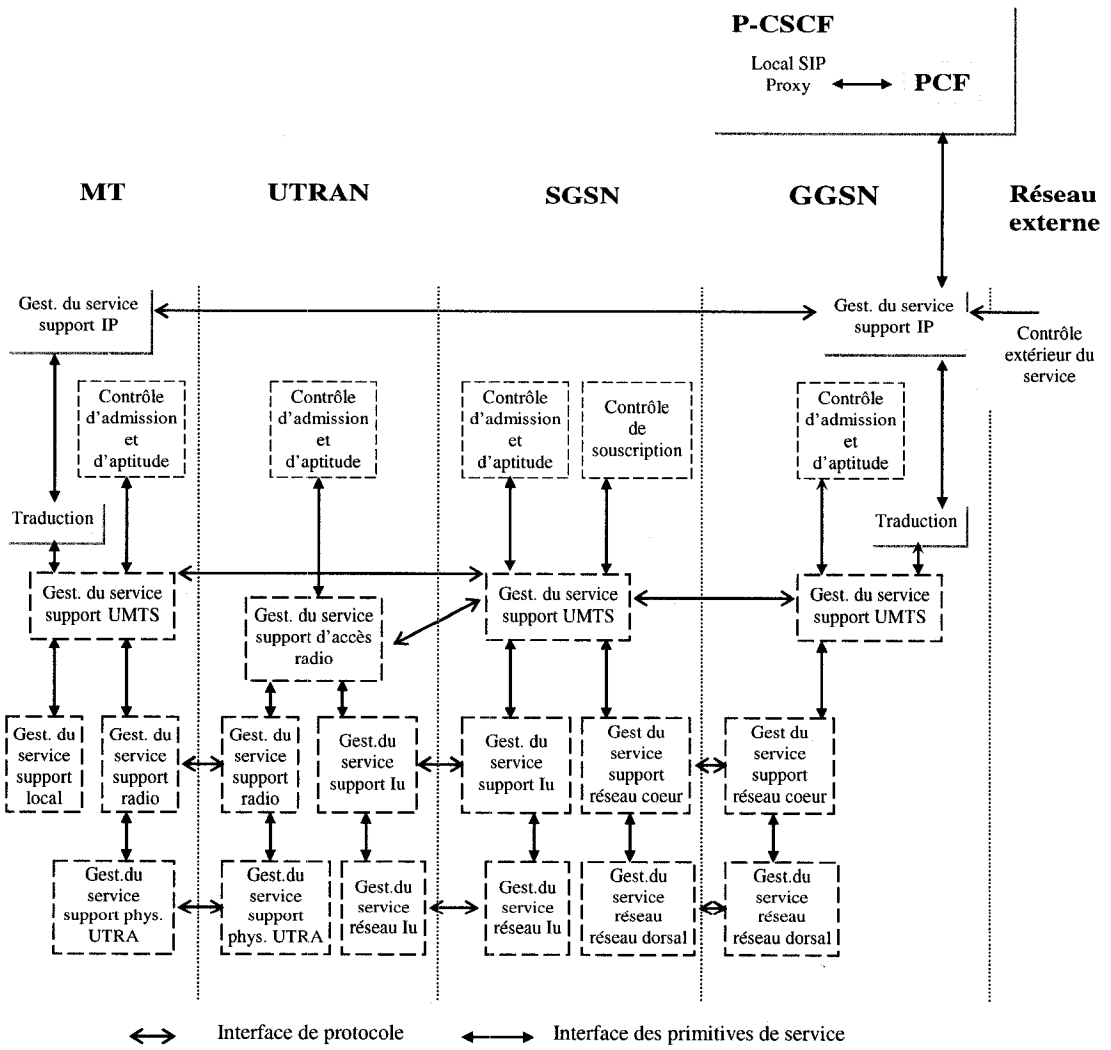

Figure 2.5 Fonctions de gestion de QdS IP (et UMTS) sur le plan de contrôle

Ce survol des fonctions de QdS IP laisse croire que les technologies existantes de QdS sont indiquées (RSVP, LDP, DiffServ, MPLS, et autres). Dans ce mémoire, l'accent est mis sur la gestion basée sur des politiques.

2.4 Cadre générique de l'IETF pour la gestion basée sur des politiques

L'approche de gestion des réseaux basée sur des politiques émane des travaux de recherche du groupe de travail *Resource Allocation Protocol* (RAP) de l'IETF [6]. Cette section est consacrée au cadre générique de l'IETF en la matière, car ce cadre se trouve à l'origine de celui de 3GPP. Elle présente l'approche d'intérêt, le protocole COPS (*Common Open Policy Service*) et son modèle dérivé COPS-PR.

2.4.1 Approche de gestion basée sur des politiques

Souvent, les domaines parcourus sont disparates, décrits par une topologie, des mécanismes de QdS et des descriptions pour les applications clairement distincts. Il n'en reste pas moins que les nœuds traversés doivent être configurés de manière cohérente. Afin de remédier à ce problème, l'IETF élabore une approche de gestion des réseaux basée sur des politiques *PBN Policy-Based Networking*. Celle-ci s'articule autour d'énoncés de la forme : *Si (condition de politique) alors (action de politique).*

Cette approche repose sur les notions de rôle, d'aptitude et de plage temporelle d'applicabilité des politiques. Elles sont liées aux nœuds du réseau dits clients de politiques. Un rôle est désigné à l'aide d'une chaîne de caractères et résume les caractéristiques qui se rattachent à un type spécifique d'élément dans le réseau, tel les interfaces et les files d'attente. Cette information administrative est exploitée par les conditions pour exprimer des données de nature politique, financière/légale, géographique, architecturale, et/ou autres. Les conditions suivantes sont données en exemple : *Si l'usager attaché appartient au groupe exécutif, Si le service payé est de type or, Si l'interface quitte l'établissement* et, enfin, *Si l'interface est de type backup.* Une plage temporelle donne la ou les périodes de validité d'une politique. Une

information d'aptitude, quant à elle, stipule que le serveur ne devrait en aucun cas installer une politique pour un élément de réseau qui serait incapable de l'exécuter. Une action de politique affecte, par exemple, un mécanisme d'ordonnancement.

Cela dit, la gestion basée sur des politiques peut servir les intérêts d'une variété de domaines (sécurité, QdS, et autres). Pour l'offre de la QdS, elle exige d'abord la conclusion d'ententes SLA entre les opérateurs pour les services de QdS IP envisagés, puis la transformation de celles-ci par chacun des opérateurs en des règles de politiques et, enfin, la traduction de ces règles en des « actions » de configuration par des entités automatisées qui connaissent les détails liés à la topologie du réseau et à ses dispositifs. De cette manière, l'opérateur peut déployer des services de QdS IP sans avoir à se soucier des particularités de son réseau.

Par ailleurs, dans l'architecture typique envisagée par l'IETF, on trouve une console *Policy Management Tool*, une centrale de dépôt *Policy Repository*, un serveur de politiques *PDP Policy Decision Point* ainsi qu'un point de renforcement des politiques *PEP Policy Enforcement Point*. Un serveur de politiques local *LPDP Local Policy Decision Point* peut assister le PEP dans ses décisions, mais celles-ci doivent être envoyées au PDP par le PEP pour approbation. L'enregistrement des politiques dans la centrale de dépôt et la configuration du point de décision sont effectués à l'aide de la console. Le serveur PDP peut posséder des interfaces de plusieurs types, notamment SNMP et LDAP. La Figure 2.6 illustre l'architecture générique de l'IETF.

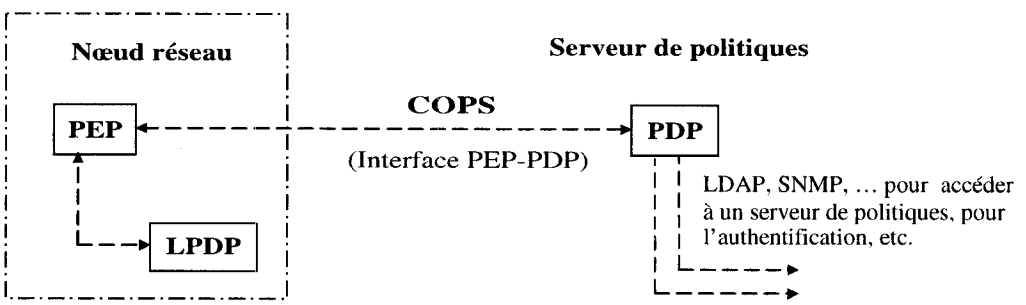

Figure 2.6 Architecture de gestion basée sur des politiques de l'IETF

Enfin, de cette gestion basée sur des politiques résulte un *contrôle d'admission basé sur des politiques* qui se fonde non seulement sur la disponibilité des ressources, mais aussi sur des politiques explicitées par l'opérateur. Le contrôle d'admission doit supporter la préemption, la tolérance aux pannes, les nœuds ignorants de politiques, les styles multiples de politiques (bilatéral, multilatéral) et la sécurité.

2.4.2 Protocole COPS

Comme indiqué à la Figure 2.6, le protocole COPS est utilisé pour véhiculer les données de politiques entre les nœuds PEP et PDP. Ci-après, le protocole et trois de ses messages sont décrits.

Description sommaire du protocole COPS

Le protocole COPS, de type requête-réponse, s'inscrit dans une architecture client-serveur. Il s'appuie sur TCP pour assurer la fiabilité de la connexion. Le client PEP peut envoyer des requêtes au serveur PDP pour quatre types d'événements: une requête d'un message entrant ou de contrôle d'admission, une requête d'allocation des ressources locales, une requête d'acheminement d'un message sortant et une requête de configuration. Les trois premiers peuvent conduire à un approvisionnement extérieur des politiques par le PEP. Il revient à l'instance de ce protocole de préciser les requêtes qui doivent forcer cette opération. En revanche, le dernier événement sollicite des données de configuration à l'avance ou lorsque des mises à jour sont souhaitées. Ces scénarios distinguent les modèles *COPS-Outsourcing* et *COPS-Provisioning*. Les décisions du PDP peuvent être synchrones ou asynchrones selon qu'elles sont corrélées directement ou indirectement à des requêtes du PEP ou liées à des événements plutôt associés au PDP. Le serveur peut aussi demander à son client de lui adresser une requête. Des messages de type « rapport » peuvent aussi être envoyés par le PEP au PDP pour l'informer du résultat d'exécution de ses décisions ou pour lui fournir des données de nature comptable. D'autres messages sont aussi prévus (connexion, etc.).

Ensuite, des fonctionnalités peuvent aisément être greffées au protocole. Il peut transporter des objets auto-identifiables et supporter des données spécifiques à des types de clients sans que sa base ne soit modifiée. Les objets auto-identifiables convoient l'information nécessaire pour indiquer l'état et le type de la requête, établir un contexte pour celle-ci, référencer des états de requêtes déjà installés, envoyer des décisions de politiques, rapporter des erreurs, fournir une intégrité niveau message et transférer des données spécifiques au client. En matière de sécurité, COPS fait l'authentification et protège contre la réplique des messages. Le canal de communication peut être sécurisé avec IPsec et TLS.

En outre, le protocole se base sur la notion d'état. Celle-ci confère à COPS une dose de flexibilité importante. Elle permet les requêtes/décisions asynchrones du PEP/PDP pour des mises à jour/modifications. Les états de requête/décision créés par le PEP sont conservés dans les deux nœuds de politiques jusqu'à ce que le client les efface explicitement. Le PDP peut solliciter la création d'un état par le PEP. Il peut se baser sur des états installés pour répondre à une requête nouvelle qui leur serait reliée. Les états liés à des événements différents peuvent être ainsi inter-associés.

Par ailleurs, afin d'assurer la tolérance aux pannes, il convient d'employer des mesures proactives et réactives de survivabilité. Entre autres, l'état de la connexion est constamment vérifié par le PEP et le PDP grâce à des échanges de messages *keep-alive*. En cas de bris de connexion, le PEP doit tenter de se connecter à nouveau au PDP ou, le cas échéant, à un PDP alternatif (de *backup*). Lors de la période de déconnexion, le PEP doit prendre des décisions localement ; il est censé notifier au PDP les états effacés et les événements ayant réussi le contrôle d'admission pendant la période grise. Donc, quand le PEP veut ouvrir une connexion pour un type de client, il doit spécifier l'adresse du dernier PDP supportant ce client qui lui a fourni des décisions persistantes. Le PDP peut aussi exiger que les états internes du PEP soient re-synchronisés, autrement dit que les requêtes déjà installées soient re-générées.

Enfin, les messages regroupent des unités atomiques de politiques. Celles-ci sont représentées à l'aide d'un modèle d'information particulier appelé *PIB*, pour *Policy*

Information Base. Un module PIB est un arbre conceptuel nommé où les branches correspondent à des structures de données génériques (classes) et les feuilles, à des instances spécifiques de celles-ci. Ces classes et ces instances portent respectivement les acronymes anglais *PRC* (*Provisioning Class*) et *PRI* (*Provisioning Instance*). Une base PIB est stockée dans tous les nœuds de politiques. Les opérations « *install* » et « *remove* » sont supportées par les instances. La première permet de créer et de mettre à jour une instance et l'autre, d'en supprimer une ou plusieurs.

Types et formats des messages et des objets COPS

Le dialogue entre les nœuds de politiques est riche de dix messages. Ceux qui nous intéressent sont les requêtes, les décisions et les rapports. Ils possèdent un en-tête et des objets. Dans l'en-tête d'un message COPS, on trouve cinq champs: un numéro de version, un drapeau, une opération, un type de client COPS (*Client-Type*) et la longueur totale du message (l'en-tête et les objets inclus). Le quatrième champ fournit un cadre d'interprétation conséquent pour les objets des messages subséquents (ex. : COPS-PR).

Après l'en-tête, on trouve les objets. Leur en-tête précise la longueur totale de l'objet, la classe C-Num de l'information et le type C-Type de la classe. Les classes C-Num définies sont *Handle*, *Context*, *In Interface*, *Out Interface*, *Reason Code*, *Decision*, *LPDP Decision*, *Error*, *Client-Specific Info*, *Keep Alive Timer*, *PEP Identification*, *Report Type*, *PDP Redirect Address*, *Last PDP Address*, *Accounting Timer* et *Message Integrity*. Les Tableaux 2.2 et 2.3 présentent ces messages et quatre de ces objets. Pour une description complète des messages et des objets, le lecteur peut se référer à l'Annexe A.6.

2.4.3 Modèle COPS-PR du protocole COPS

Le modèle *COPS-Provisioning* constitue une instance du cadre générique de l'IETF sur le protocole COPS. Il est décrit ci-après parce que celui de 3GPP en découle.

Tableau 2.2 Formats des messages *Request*, *Decision* et *Report* de COPS

Formats des messages COPS-Req, COPS-De et COPS-Rpt		
<Request> :: =	<Common Header> <Client Handle> <Context> [<IN-Int>] [<OUT-Int>] [<ClientSI(s)>] [<LPDPDecision(s)>] [<Integrity>] <ClientSI(s)> :: = <ClientSI>|<ClientSI(s)> <ClientSI>	<LPDPDecision(s)>:: = <LPDPDecision>|<LPDPDecision(s)> <LPDPDecision> <LPDPDecision> ::= [<Context>] <LPDPDecision: Flags> [<LPDPDecision: Stateless Data>] [<LPDPDecision: Replacement Data>] [<LPDPDecision: ClientSI Data>] [<LPDPDecision: Named Data>]
<Decision> :: =	<Common Header> <Client Handle> <Decision(s)>|<Error> [<Integrity>] <Decision(s)> :: = <Decision>|<Decision(s)> <Decision>	<Decision> :: = <Context> <Decision: Flags> [<Decision: Stateless Data>] [<Decision: Replacement Data>] [<Decision: ClientSI Data>] [<Decision: Named Data>]
<Report State>:: =	<Common Header> <Client Handle> <Report-Type> [<ClientSI>] [<Integrity>]	

Note : Après l'en-tête, les objets dans les opérateurs <> sont obligatoires et [< C-Num : C-Type >].

Description sommaire du protocole COPS-Provisioning (COPS-PR)

Le modèle *COPS-Provisioning* est aussi dénommé *COPS-Configuration*. Dans ce modèle, les requêtes décrivent le PEP et ses paramètres de configuration [7]. Elles sont émises pour solliciter une configuration au départ ou sur détection d'un changement interne au PEP (défectuosité d'interface, etc.). Elles sont donc beaucoup moins fréquentes. Les décisions du PDP sont généralement envoyées pour réagir à des événements externes ou survenus dans le PDP, tels que des mises à jour dans la centrale de dépôt de politiques ou dans les ententes SLA. Les messages COPS susmentionnés

sont supportés, mais les formats des messages *COPS-Req*, *COPS-Dec* et *COPS-Rpt* changent, comme on peut le constater dans le Tableau 2.4.

Tableau 2.3 Description des objets *Handle*, *Context* et *Client-Specific Info*

Objet	*Description*
Handle C-Num = 1 C-Type = 1	- Cet objet de longueur variable est l'identifiant d'un état de requête/décision dans le PEP et le PDP. Il est mis dans les requêtes, les décisions, les rapports, les messages de synchro. et de suppression d'état.
Context C-Num = 2 C-Type = 1	- Cet objet indique le type de l'événement qui a déclenché la requête et conditionne la décision du PDP (quant aux objets à inclure).
Decision C-Num = 6	- Cet objet est généré par le PDP et inséré dans des réponses. Ses champs obligatoires dépendent du type de client et de la décision. → C-type = 1, drapeaux (*decision flags*) ⇐ obligatoire et/ou → C-type = 2, donnée sans état (*stateless data*) ou → C-type = 3, donnée de substitution (*replacement data*) ou → C-type = 4, donnée spécifique client (*client-spec. decision data*) ou → C-type = 5, donnée nommée de décision (*named decision data*) - Les formats des quatre derniers objets dépendent du type de client.
Client-Specific Information (ClientSI) C-Num = 9	- Cet objet peut être inséré dans les requêtes, les rapports et les messages d'ouverture pour fournir une donnée spécifique au client. → C-type = 1, inform. signalée spécifique au client *Signaled ClientSi* → C-Type = 2, information nommée de configuration *Named ClientSi*.

Ces messages changent de format pour intégrer de nouveaux objets (liés aux erreurs ou nommés après). Ils sont insérés dans l'objet *Named ClientSI* des messages COPS-Req et COPS-Rpt et dans l'objet *Named Decision Data* de COPS-Dec. Les champs S-Num et S-Type de leur en-tête remplacent leurs champs similaires C-Num et C-Type de COPS. Dans l'Annexe A.7, ces objets sont définis et leur format est donné. De plus, l'opération « *install* » spécifie deux nouveaux paramètres de COPS-PR : le *PRID Provisioning Instance Identifier* et le *EPD Encoded Provisioning Instance Data*. Le PRID constitue l'identifiant de l'instance et est unique pour un *Client-Type* et un état de requête donnés. Le EPD renferme les valeurs nouvelles ou mises à jour des attributs

de l'instance. L'opération « *remove* » spécifie le PRID de l'instance à effacer ou le préfixe *PPRID Prefix PRID* d'un ensemble de classes.

Tableau 2.4 Messages convoyant de l'information spécifique au type de client

< Request > :: =	< Decision Message > :: =	< Report State > :: =
<Common Header> <Client Handle> <Context = config request> *(<Named ClientSI>) [<Integrity>]	<Common Header> <Client Handle> *(<Decision>)| Error> [<Integrity>] <Decision> :: = <Context> <Decision: Flags> [<Named Decision Data: Provisioning >]	<Common Header> <Client Handle> <Report Type> *(<Named ClientSI>) [<Integrity>]

Cela dit, malgré les vertus du modèle COPS-PR, il a pour lacune, selon 3GPP, d'empêcher l'approvisionnement extérieur des politiques à des moments opportuns.

2.5 Cadre générique de 3GPP pour la gestion basée sur des politiques

Dans le but de profiter des scénarios de configuration et d'approvisionnement extérieur de politiques, 3GPP déclare « événements d'approvisionnement » les requêtes d'activation et de modification de contexte. Cette section explore d'abord le cadre générique de 3GPP sur la gestion basée sur les politiques locales des services SBLP (*Service-based Local Policy*), puis explique les procédures du protocole de l'extension proposée. Après avoir présenté des mises en correspondance essentielles, elle développe le processus d'établissement de session.

2.5.1 Description sommaire

Le cadre générique de 3GPP est donc similaire à celui de l'IETF, à quelques détails près. Il supporte huit interactions sur l'interface Go. Celles-ci peuvent autoriser

les ressources, les réserver, accepter l'allocation des ressources autorisées, les refuser et annuler l'autorisation des ressources [9, 10]. Elles peuvent, en outre, indiquer la libération du contexte PDP (PEP→PCF), autoriser la modification de celui-ci et annoncer sa modification (PEP→PCF). Elles sont nommées, dans l'ordre, *Authorize QoS Resources*, *Resource Reservation*, *Approval of QoS Commit* (ex.: 'open gate'), *Removal of QoS Commit* (ex. : 'close gate'), *Revoke Autorisation*, *Indication of PDP Context Release*, *Authorization of PDP Context Modification*, *Indication of PDP Context Modification*. L'Annexe A.8 présente l'extension, c'est-à-dire le module PIB 3GPP Go. Les objets ajoutés permettent de traiter les événements qui requièrent une interaction avec le PCF, les décisions qui leur sont relatives, la terminaison de ceux-ci et leur utilisation des ressources.

2.5.2 Procédures du nouveau protocole

Les interactions susnommées sont englobées dans les procédures d'initialisation du PEP, de configuration de celui-ci et d'approvisionnement extérieur des politiques [9, 10, 11]. Les procédures sont ci-après explorées.

Procédure de requête d'initialisation du PEP

Le PEP établit la connexion TCP avec le PCF en écoutant sur son port serveur 3288. Il forme ensuite avec lui une association de sécurité, puis transmet un message *Client-Open* qui inclut, entre autres, le *Client-Type* COPS-PR et l'adresse du dernier PCF (du *Client-Type*) lui ayant fourni des décisions persistantes. Le PDP peut accepter ou refuser la connexion. Le message *Client-Close* libère les ressources.

Procédure de requête de configuration du PEP

Le PEP envoie une requête de configuration au PCF afin de créer un état dans celui-ci. Il indique ses aptitudes, c'est-à-dire les structures des modules PIB DiffServ et 3GPP Go ainsi que d'autres données spécifiques au client, soient le type de matériel, la

version de logiciel et la configuration actuelle. Il mentionne la combinaison des rôles de ses interfaces et, s'il le désire, le type de signalisation qu'il met à la disposition du PCF pour le service de support. À l'aide des aptitudes spécifiées et des politiques indexées pour la requête, le PCF génère une décision et l'envoie au PEP. Celle-ci stipule les politiques qui doivent être configurées dans le PEP, c'est-à-dire les types d'événements qui devront conduire à un approvisionnement extérieur des politiques. La décision peut aussi fournir l'information de configuration pour les gérer et celle pour traiter les autres événements. Le PEP les traduit ensuite en actions de configuration locales.

Procédure d'approvisionnement extérieur des politiques

Après la procédure de configuration, le point de renforcement peut gérer les événements de politiques. Sur réception d'une requête de création/modification de contexte PDP, le PEP du GGSN détermine l'adresse du PCF à l'aide du jeton et lui envoie un message *UMTS Service Request*, lequel renferme à la fois le jeton et l'identificateur de flot dans l'objet *Client specific*. Le PCF tente ensuite de corréler cette requête avec un état d'autorisation dans sa base de données. S'il parvient à le faire, il envoie un message *Outsourced UMTS Decision* pour dire au PEP de réserver les ressources requises. Le PEP exécute la décision et répond au PCF avec un message *UMTS Service Usage Report*. Les messages de type *Update PDP Context Request* sont générés sur réception d'une requête de modification par le GGSN. Le PCF peut envoyer des messages *Outsourced UMTS Decision* de manière asynchrone (pour allouer les ressources par exemple) et le PEP peut transmettre des notifications au PCF grâce aux messages *UMTS Service Usage Reports*. Si le GGSN reçoit une requête *Delete PDP Context Request*, son PEP doit transmettre au PCF un message *UMTS service Usage Termination* pour supprimer l'état installé dans le PCF. Enfin, ces procédures sont utilisées pour établir une session avec IMS.

2.5.3 Mises en correspondance

Le processus d'établissement de session implique des mises en correspondance dans les nœuds usager, GGSN et PCF. Les attributs manipulés sont la classe de QdS et les débits des voies montante et descendante [9, 10]. Ces conversions sont expliquées ci-après.

Dans le PCF, les paramètres SDP de l'usager sont transformés en paramètres de QdS IP autorisés. Les données IP sont précisées dans les politiques d'une centrale de dépôt et les attributs SDP sont fournis au PCF par le P-CSCF. Dans l'usager, les paramètres de l'application sont mis en correspondance avec ceux du gestionnaire de ressources IP s'il est supporté, puis avec ceux du gestionnaire de ressources UMTS pour tous les flots IP de la session. Si les politiques SBLP sont appliquées, l'usager devrait convertir les paramètres SDP en paramètres de QdS autorisés afin d'en tenir compte. Dans la passerelle GGSN, une mise en correspondance et une comparaison sont effectuées. Les attributs de QdS IP autorisés par le PCF sont d'abord transformés en attributs de QdS UMTS autorisés. Ensuite, les paramètres de QdS UMTS autorisés sont comparés aux paramètres de QdS UMTS indiqués dans la requête d'activation ou de modification de contexte envoyée par l'usager. Deux conditions doivent être remplies pour que la requête soit acceptée : ① l'attribut demandé *Guaranteed Bitrate* (*Maximum bitrate*) *DL/UL* de l'application conversationnelle / à flux continu (interactive / en arrière plan) doit être inférieur ou égal à l'attribut *Maximum Authorized data rate UL/DL* et ② la classe de trafic demandée doit être inférieure ou égale à celle autorisée (*Maximum Authorized Traffic Class*).

Ces mises en correspondance utilisent les règles données à l'Annexe A.9. Après la dernière conversion, la décision du réseau cœur est connue.

2.5.4 Processus d'établissement d'une session multimédia

Le processus d'établissement de session utilise donc un nouveau protocole et une série de mises en correspondance. Il inclut les phases d'autorisation, de réservation et

d'allocation des ressources [9, 10, 11]. Nous décrivons maintenant ce processus pour une session multimédia ou de voix sur IP acceptée entre deux usagers situés dans le même domaine. Il est montré à la Figure 2.7

Après s'être attaché au réseau, l'usager active un contexte PDP pour la signalisation IMS et s'enregistre dans le S-CSCF du sous-système multimédia. Ensuite, il peut commencer la phase d'autorisation des ressources. D'abord, il transmet les paramètres SDP dans un message INVITE qu'il envoie au destinataire. Sur réception de ce message, celui-ci fait un choix de paramètres pour la session et le donne au P-CSCF qui le dessert. Ce dernier soumet à sa fonction de contrôle les attributs SDP pertinents, attributs à l'aide desquels celle-ci indexe et télécharge des politiques d'une centrale de dépôt. Après avoir déterminé les paramètres IP autorisés pour la session, elle génère un jeton d'autorisation (*Authorization Token*) et le transmet, via le P-CSCF, par le même chemin, à l'usager d'origine. Du côté source, le P-CSCF envoie les informations qu'il reçoit à la fonction PCF. Celle-ci effectue les mêmes opérations, c'est-à-dire elle indexe les politiques pertinentes à partir d'une centrale de dépôt, les télécharge, génère un jeton d'autorisation et l'envoie via le P-CSCF à l'usager concerné. Ce processus d'autorisation de qualité de service (*Authorize QoS Request*) peut s'avérer itératif.

Ensuite, la réservation des ressources peut être effectuée à l'origine et à la destination grâce à des requêtes d'activation de contexte PDP qui incluent l'information de corrélation. Sur réception de cette requête, le PEP du GGSN extrait le jeton d'autorisation et les identificateurs de flots pertinents, et les transmet dans une requête COPS-PR au PCF. À l'aide des informations reçues, le serveur essaie de corréler la requête pour la session à un état d'autorisation dans sa base de données. S'il parvient à valider la requête, il génère une décision COPS-PR qu'il adresse au point de renforcement PEP. Celle-ci renferme, au minimum, la décision de corrélation (si elle a été trouvée), la QdS autorisée et la porte *gate*. Elle dit de réserver les ressources requises. La passerelle GGSN envoie la réponse à l'usager dans un message *PDP Context Activation Response*. La réservation des ressources se fait des deux côtés en parallèle, c'est-à-dire à l'origine et à la destination.

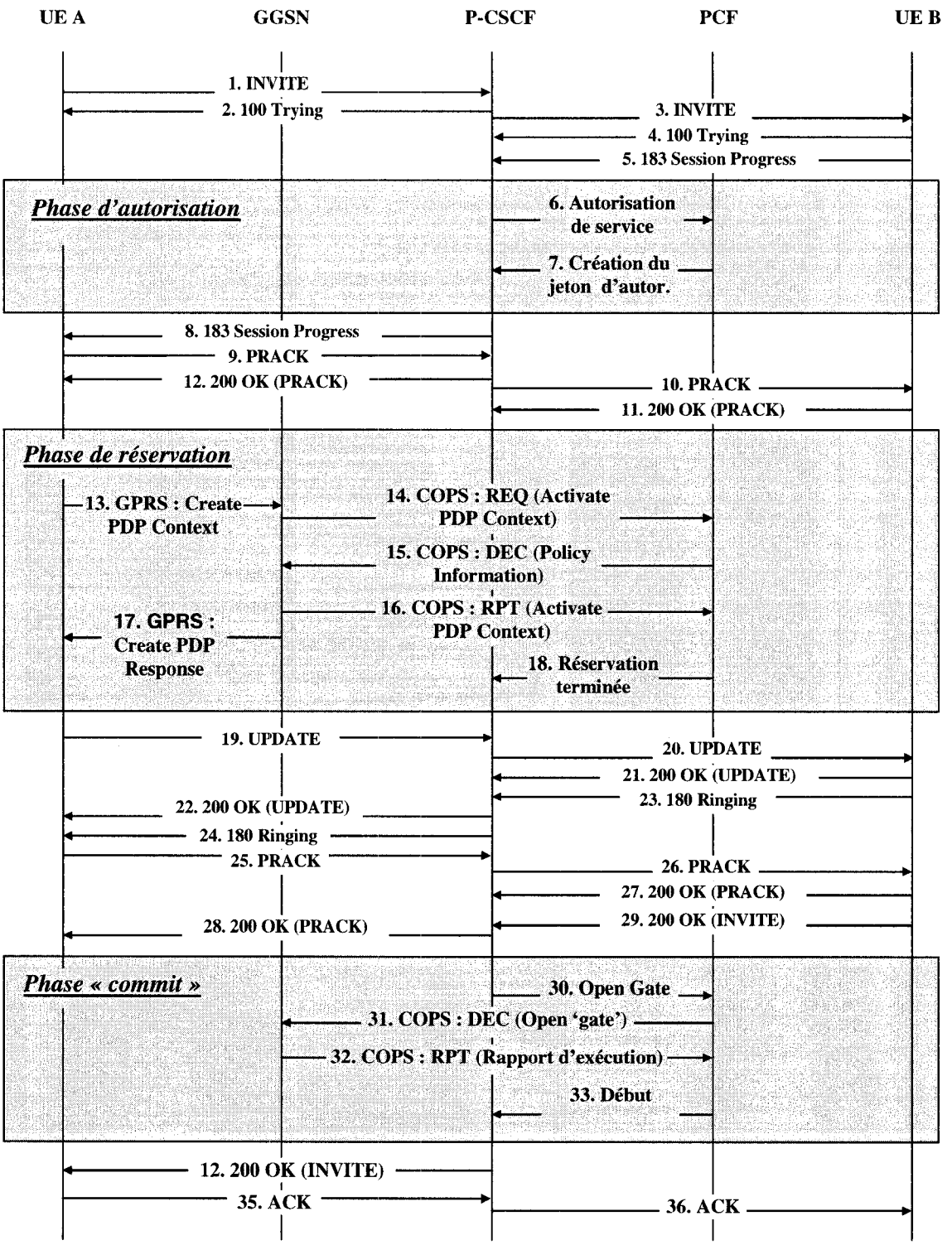

Figure 2.7 Processus d'établissement d'une session multimédia entre deux usagers

En ce qui concerne la phase d'allocation des ressources, elle est déclenchée après que l'usager de destination a entendu la sonnerie. Celui-ci envoie un message SIP 200 OK à l'usager d'origine. Le P-CSCF de destination, en l'interceptant, signale le PCF qui génère aussitôt une décision COPS ordonnant au PEP d'ouvrir la porte *gate* des flots IP concernés. Ce message SIP donne lieu à l'ouverture de la porte *gate* du côté source. Quand l'usager reçoit le message SIP 200 OK, la session est créée. Dans le schéma ci-haut, les étapes d'initialisation et de configuration du PEP ne sont pas montrées. Pour conclure, la gestion basée sur des politiques permet d'éclaircir le problème de contrôle de congestion des réseaux UMTS.

2.6 Mécanismes de contrôle d'admission basés sur des mesures

Après avoir étudié les cadres génériques de 3GPP et de l'IETF sur la gestion basée sur des politiques, il convient maintenant de faire état des solutions de la littérature qui se rattachent au volet « disponibilité des ressources » de ce mémoire, c'est-à-dire de traiter du module proactif de contrôle de congestion censé contribuer à l'approche de gestion de 3GPP. Cette section commence par vulgariser les notions d'auto-similarité, de dépendance à long terme et de distributions à queue lourde. Elle définit ensuite l'application d'ingénierie de trafic d'intérêt. Après, elle discute des mécanismes de contrôle d'admission basés sur des mesures et détaille deux instances de ces modules. Elle fournit, à la fin, une mise en contexte pour UMTS.

2.6.1 Auto-similarité, dépendance à long terme et distributions à queue lourde

Les distributions à queue lourde et les concepts d'auto-similarité et de dépendance à long terme (LRD) se trouvent au cœur de la modélisation du trafic. Ci-après, nous fournissons les définitions mathématiques pour ces notions et indiquons les causes et évidences des nouvelles propriétés du trafic. Des résultats d'études importants sont aussi mentionnés.

Cadre théorique pour l'auto-similarité, la dépendance à long terme et les distributions à queue lourde

L'auto-similarité, la dépendance à long terme et les distributions à queue lourde sont importantes dans le domaine de la modélisation du trafic. Leurs définitions mathématiques sont bien connues [12, 13, 14, 23]. En ce qui concerne la première notion, c'est sa définition asymptotique qui nous intéresse – par rapport aux autres définitions de ce concept. Ainsi, soit un processus stationnaire au sens large $X = (X_t: t = 1, 2, 3, \ldots)$ et sa série m-agrégée $X_k^{(m)}$ [12, 13, 14, 23]:

$$X_k^{(m)} = \frac{1}{m}\left(X_{km-m+1} + \ldots + X_{km}\right) \qquad k = 1, 2, 3, \ldots$$

Ce processus est dit asymptotiquement auto-similaire de second ordre et de paramètre H si la variance et la fonction d'auto-corrélation de la série agrégée sont identiques à celles de la série originale pour des plages temporelles k suffisamment grandes et une taille m de l'agrégat qui tend vers l'infini (moyennant un changement d'échelle), c'est-à-dire [12, 13, 14, 23]:

$$Var\left(X^{(m)}\right) = Var(X)/m^{\beta} \quad (1) \quad \text{et} \tag{2.1}$$

$$r_{X^{(m)}}(k) = r_X(k) \text{ pour } 0 < \beta < 1 \text{ et m} \rightarrow \infty \tag{2.2}$$

Conséquemment, pour un processus auto-similaire [12, 13, 14, 23],

- ✓ la variance décroît de manière hyperbolique lorsque m tend vers l'infini ;
- ✓ la fonction d'auto-corrélation décroît de manière hyperbolique lorsque m tend vers l'infini et $\sum_k r(k) = \infty \rightarrow$ dépendance à long terme et
- ✓ la densité spectrale suit une distribution à queue lourde près de l'origine.

Ensuite, le degré d'auto-similarité d'un processus est déterminé par la valeur de son paramètre de Hurst H, avec $H = 1 - \beta/2$ et $½<H<1$. Pour un trafic ayant une

dépendance à court terme, H est égal à ½ et β est égal à l'unité. L'auto-similarité et la dépendance à long terme augmentent avec la valeur de ce paramètre.

En outre, les distributions à queue lourde sont intimement liées à l'auto-similarité et à la dépendance longue mémoire. Un processus X est dit à queue lourde si [12, 13, 14, 23]:

$$P[X > x] \sim x^{-\alpha} \qquad \text{lorsque } x \to \infty,\ 0<\alpha<2$$

Pour ce processus, si $\alpha \leq 2$, la variance est infinie et si $\alpha \leq 1$, la moyenne est aussi infinie. Lorsque α décroît, la queue de la distribution se voit attribuer une plus grande portion de la probabilité de masse.

Afin de témoigner de l'auto-similarité d'un processus, plusieurs tests ont été développés. Les méthodes évaluent le paramètre H et incluent le graphe variance-temps, le graphe R/S, la méthode du périodogramme et l'estimateur de Whittle. À titre indicatif, le premier test est fondé sur l'équation (1). Il donne, en coordonnées log-log, la variance du processus agrégé $X_k^{(m)}$ en fonction de la taille m de l'agrégat. Le paramètre est donc estimé à partir de la pente du graphique (la pente égale $2H - 1$).

Cela dit, la génération synthétique des traces de trafic auto-similaire [3, 12, 13, 14, 23] peut être basée sur des méthodes exactes ou sur la superposition de sources ON/OFF à queue lourde. En effet, l'agrégation de ces sources conduit à un trafic de dépendance longue mémoire [12, 13, 14, 23]. En fait, une série de modèles ont été définis (fractales, ondelettes, etc.) pour décrire les sources LRD ; il peuvent modéliser la source, le tampon, le comportement des protocoles adaptatifs (TCP, UDP), le comportement de l'usager, etc. [3]. Néanmoins, malgré les efforts consentis par la recherche en ce sens, les modèles actuels de trafic sont le plus souvent inadéquats.

Interprétation intuitive de l'auto-similarité et de la dépendance à long terme

D'un point de vue intuitif, l'auto-similarité et la dépendance à long terme se traduisent par des fluctuations dans le trafic grandes en amplitude et persistantes sur

plusieurs échelles de temps. Contrairement au trafic de Poisson, le trafic présente des corrélations significatives sur ces échelles. En conséquence, les résultats qui découlent des hypothèses markoviennes ne peuvent pas être utilisés.

Évidences et causes de l'auto-similarité et de la dépendance à long terme

À l'aide de l'un ou l'autre de ces tests, plusieurs caractéristiques inhérentes au trafic ont été prouvées auto-similaires. À titre d'exemple, nous pouvons donner les temps de transmission (ON) web, les temps de silence (OFF) web, les inter-arrivées des requêtes web, les temps d'inter-arrivée des paquets TCP, les arrivées des connexions TCP, le nombre de connexions TCP par session web, les inter-arrivées des paquets Telnet, les tailles des rafales FTP, la durée des sessions, les pertes de paquets, la taille des trames vidéo, etc [15, 16, 17, 18, 19, 20, 21, 22]. Mais, les sources vidéo à débit variable sont intrinsèquement auto-similaires. Ces nouvelles distributions sont imputables aux flux multimédias dits éléphants.

De manière générale, les causes de l'auto-similarité sont reliées à l'application/l'usager ou encore au système/réseau. Par exemple, si le processus de cache est efficace, la variabilité de la taille des fichiers disponibles peut être la cause première du comportement excentrique du trafic web. Le temps de réflexion de l'usager est une autre cause. Pour le trafic vidéo, l'auto-similarité peut être imputable à un patron périodique GOP et aux différentes tailles pour les trames – la taille dépend surtout de la nature (I, P, B) de la trame et du niveau d'activité de la scène.

En outre, certains protocoles génèrent un trafic auto-similaire. Mais, les échelles de temps sont nettement inférieures, de la durée d'une rafale ou de l'ordre de un RTT à plusieurs centaines de RTT (au plus sur quatre ordres de grandeur). En fait, la contribution des protocoles adaptatifs à l'auto-similarité peut être expliquée par les rafales qu'ils produisent [16]. Par exemple, UDP peut en créer par la fragmentation. Le protocole TCP peut, dans des conditions sévères de congestion, devenir chaotique et générer de l'auto-similarité sur de courtes échelles de temps. En effet, les phases *slow start*, *fast retransmit* avec *loss recovery*, *congestion avoidance* et *exponential backoff* y

concourent [16, 17, 18]. Enfin, comme exemples supplémentaires de causes de rafales, citons la compression ACK, les failles d'implémentation du *idle restart timer*, les ACK cumulatifs ou perdus ou encore la nature sporadique des applications [16]. Quoi qu'il en soit, les recherches sur les causes d'auto-similarité demeurent prolifiques.

Quelques résultats d'études

Nombreuses sont les études qui ont évalué l'impact de l'auto-similarité et de la dépendance à long terme sur la performance des réseaux [15, 16, 17, 18, 19, 20, 21, 22, 23]. Certains résultats sont particulièrement intéressants. Entre autres, le comportement d'échelle à long terme importe aux niveaux d'utilisation élevés, par opposition au comportement aux échelles fines qui affecte la performance des files d'attente aux niveaux d'utilisation modérés. Ensuite, le degré d'auto-similarité croît avec le niveau d'utilisation du réseau et les pertes induites par un trafic auto-similaire sont supérieures à celles induites par un trafic de Poisson. De plus, l'augmentation de l'utilisation des liens pour un service non-orienté connexion nécessite une augmentation démesurée de la taille des tampons. En outre, la distribution pour la taille de la file d'attente suit une loi de Weibull (queue lourde) de sorte que l'emploi des modèles de contrôle de congestion basés sur les modèles traditionnels peut donner lieu à une sous-estimation considérable des pertes. Les délais dans ces files sont aussi accrus. En outre, une étude [3] indique que les fluctuations lentes par rapport à la durée moyenne d'un flot peuvent être absorbées par les changements dans le nombre de flots dans le système, tandis que les fluctuations rapides doivent être absorbées par une augmentation de la capacité. Pour une échelle donnée, elle propose donc l'existence d'un horizon au-delà duquel les caractéristiques d'auto-similarité du trafic observées aux échelles supérieures n'ont pas d'effet sur l'échelle examinée.

Généralement, les diverses méthodes de contrôle de congestion s'exécutent à des échelles de temps différentes, courtes, moyennes et longues. Les échelles qui s'étalent sur des heures, des journées et des mois sont employées pour des activités telles que le dimensionnement des réseaux, la description des ententes SLA et l'identification des

problèmes persistants de congestion (ex. : *hotspots*). Les échelles inférieures comportent celle du paquet de l'ordre des millisecondes (ordonnancement des paquets), celle de la rafale de l'ordre des secondes (gestion des tampons) et celle de la session (période RTT) pouvant durer des minutes ou des heures. Le module de contrôle principal pour la dernière échelle est le mécanisme de contrôle d'admission. Les méthodes de contrôle à ces échelles peuvent agir de manière concurrente même si elles concourent toutes aux objectifs d'ingénierie de trafic.

2.6.2 Généralités sur les mécanismes de contrôle d'admission

Dans le but de trouver un compromis acceptable entre le niveau d'utilisation des ressources et le niveau de QdS offert aux applications, un système d'ingénierie de trafic est censé inclure des mécanismes de contrôle de congestion. Un mécanisme de contrôle d'admission est un module de contrôle proactif, car il évalue les ressources requises par les connexions (et la requête) et choisit d'accepter ou de refuser une requête en fonction d'un critère de décision préétabli. Ci-après, des généralités sont données sur ces modules et les mécanismes basés sur des mesures sont détaillés.

Généralités sur les mécanismes de contrôle d'admission

Un mécanisme de contrôle d'admission intègre un processus de mesure, des descripteurs de trafic (par ex., token bucket) et un critère d'admission. Si les descripteurs sont adéquats, le processus de mesure peut être supprimé ; auquel cas on obtient un mécanisme de contrôle d'admission basé sur des paramètres dit *PBAC,* pour *Parameter-Based Admission Control.* Celui-ci est de nature stochastique ou déterministe (taux maximum ou pire cas). Dans le cas contraire, où les descripteurs de trafic seraient inadéquats et où le processus de mesure serait obligatoire pour rendre compte de l'état réel du réseau, on aurait un mécanisme de contrôle d'admission basé sur des mesures, c'est-à-dire un module *MBAC* (*Measurement-Based Admission Control*). Si les mécanismes de contrôle d'admission basés sur des mesures sont incapables de

fournir des garanties de QdS, ils peuvent s'adapter au réseau et pallier les modèles inadéquats de trafic. Ils sont donc préconisés pour les réseaux UMTS [3, 24].

Mécanismes de contrôle d'admission basés sur des mesures

Dans le schéma fonctionnel d'un mécanisme de contrôle d'admission basé sur des mesures, on trouve un estimateur et un critère de décision. Le premier sous-module calcule les ressources requises en se basant sur les besoins des connexions actuelles et, possiblement, sur les descripteurs du nouveau flot. Le second émet une décision en fonction des besoins des flots en cours et de la requête. Les mesures correspondent, entre autres, au niveau d'utilisation d'un lien, à la probabilité de saturation d'un tampon ou encore au délai de bout-en-bout à travers le réseau. Dans ce mémoire, nous nous intéressons au premier type de mesure, plus particulièrement, à la largeur de bande effective. Celle-ci est égale au quotient de la largeur de bande totale requise pour respecter les contraintes de QdS des flots multiplexés et une ressource tampon donnée sur le nombre de sources de trafic multiplexées [11]. Les mécanismes de contrôle d'admission basés sur des mesures sont de toutes natures. Les paramètres estimés, la méthode de collecte des mesures (par lien, par classe, par flot), les descripteurs requis pour le nouveau flot sont des éléments de différenciation entre les MBAC.

Dans tous les cas, le degré de performance de ces modules est lié à leur estimateur, à leur critère de décision ou encore à la combinaison de ces deux sous-modules. Certains estimateurs utilisent des algorithmes classiques et mettent à la place des valeurs dérivées des descripteurs celles qui sont obtenues à partir des mesures. Ils sont dits basés sur l'hypothèse de certitude d'équivalence (*Certainty Equivalence*). C'est le cas, entre autres, des estimateurs basés sur les bornes de Chernoff et de ceux basés sur la théorie de déviation large [11]. Si les estimateurs CE ont l'avantage de récupérer la structure des mécanismes classiques, ils font l'erreur souvent fatale d'ignorer l'incertitude inhérente aux mesures et d'accepter trop souvent un surcroît de requêtes. Plusieurs algorithmes essaient de pallier cette lacune: par exemple, certains font usage d'une procédure conservatrice de mesure et d'autres caractérisent l'erreur

[11]. Par ailleurs, plusieurs critères de décision existent. Certains d'entre eux incorporent les résultats des décisions précédentes de contrôle d'admission. Par exemple, le critère *P-T Policy-Target* peut définir un seuil sur le nombre de flots multiplexés pour un type donné. Le critère *P-TO*, ou *Policy Threshold*, détermine un seuil limite. Le critère *P-BP Policy Back-Off Period* stipule implicitement que le nombre d'erreurs peut être inacceptable en présence de haute charge et, ce, même si la probabilité d'une erreur d'admission est faible. Si un flot donné est rejeté, l'algorithme attend le départ du système d'un flot de son type avant d'admettre une requête du type du flot rejeté.

2.6.3 Algorithmes AC-MVE et AC-KQ de la littérature

En vue de déterminer la largeur de bande effective d'un lien, plusieurs algorithmes estiment les statistiques de moyenne et de variance à l'aide d'une série d'échantillons de mesures [11]. À titre d'exemple, citons les mécanismes *AC-MVE* et *AC-KQ* qui ne formulent pas l'hypothèse de certitude d'équivalence et bornent, d'une manière ou d'une autre, le taux de perte. Les acronymes correspondent respectivement aux dénominations anglaises *Admission Control based on Mean Variance* et *Admission Control based on Traffic Envelope*. Ces algorithmes sont ici décrits.

En ce qui concerne le mécanisme AC-MVE, il combine l'estimateur *Mean-Variance E-MVE* et le critère de décision *Policy-Threshold P-TO*. La disponibilité des ressources est vérifiée sur une échelle de temps unique. La largeur de bande effective E est évaluée avec la moyenne $\bar{x}$, l'écart-type σ et le paramètre α' comme suit:

$$E = \bar{x} + \alpha' \sigma$$

La moyenne capture les changements à long terme de l'agrégat de trafic multiplexé tandis que la variance caractérise la variabilité de l'agrégat sur l'échelle de temps des mesures. Le paramètre α' permet d'accommoder l'erreur d'échantillonnage qui est imputable au caractère aléatoire des mesures, de même que les fluctuations qui

sont observées sur plusieurs échelles de temps (LRD). La valeur α' est une correction apportée à un paramètre α déterminé par l'usager. Elle implique que l'erreur possède les propriétés d'une loi normale. La valeur α' est ainsi obtenue à l'aide de α et du nombre T d'échantillons de mesures:

$$\alpha' = \max \left\{ \alpha, \sqrt{(T+1)\left(e^{\alpha^2/T} - 1\right)} \right\} \tag{2.3}$$

Cet estimateur peut, à une échelle de temps petite, donner lieu à une sous-estimation des ressources requises pour satisfaire les besoins en QdS. Le critère de décision de ce mécanisme de contrôle d'admission est trivial. Pour accepter la requête, il vérifie si la valeur estimée pour la largeur de bande est inférieure à la capacité C du lien, c'est à-dire :

$$\bar{x} + \alpha'\sigma \leq C \tag{2.4}$$

En ce qui concerne l'algorithme AC-KQ, il combine l'estimateur *Traffic Envelope E-KQ* et le critère de décision *Policy-Threshold P-TO* [3]. Son estimateur caractérise le trafic sur plusieurs échelles de temps afin de capturer l'ensemble de ses fluctuations, à court terme et à long terme. Il considère une période de base τ et des échelles de temps I_η multiples de τ $I_{1,2,...}$ = 1, 2, ... x τ. À l'intérieur d'un intervalle $[s, s + I_\eta]$, le taux d'un lien est décrit par [3]:

$$X[s, s + I_\eta] / I_\eta$$

Le taux maximal pour n'importe quel intervalle est donc [3] :

$$R_\eta = \max_s X[s, s + I_\eta]$$

Sur un intervalle élémentaire, c'est-à-dire de longueur τ , l'activité est [3]:

$$x_t = X[t, (t+1)] \times \tau$$

Aussi, à partir de l'instant t, pour les T plus récents intervalles élémentaires et pour une valeur η donnée, on obtient une valeur de l'enveloppe maximale R_η^1 [3]:

$$R_\eta^1 = \frac{1}{\eta\tau} \max_{t-T+\eta \le s \le t} \sum_{u=s-\eta+1}^{s} x_u$$

Des enveloppes de trafic sont déterminées pour η = 1, 2, ... T. Avec cette formule, on évalue des enveloppes à chaque t τ secondes. On cherche à obtenir n enveloppes de trafic pour η = 1, 2, ...T et n = 1, ...N. De cette manière, on trouve la moyenne empirique $\overline{R_\eta}$ et la variance σ_η^2 [3]:

$$\overline{R_\eta} = \sum_{m=1}^{m=M} \frac{R_\eta^m}{M} \qquad \text{et} \qquad \sigma_\eta^2 = \frac{1}{m-1} \sum_{m=1}^{m=M} \left(R_\eta^m - \overline{R_\eta}\right)^2$$

Les M enveloppes consécutives caractérisent le trafic à long terme. Cela dit, l'estimateur calcule la largeur de bande à long terme et à court terme [3]:

$$E_{long} = \overline{R_T} + \alpha_{long}\,\sigma_T \tag{2.5}$$

$$E_{short} = \max_{\eta=1,2,\ldots,T} \left\{ \frac{\left(\overline{R_\eta} + \alpha_{short}\,\sigma_T\right)\eta\tau}{\eta\tau - \frac{q}{C}} \right\} \quad \text{avec} \tag{2.6}$$

$$\alpha_{long} = Q^{-1}\left(\frac{\varepsilon \overline{R_T}}{\sigma_T}\right) \tag{2.7}$$

$$\alpha_{short} = Q^{-1}\left(\frac{\varepsilon \overline{R_T}}{\sigma_\eta}\right) \tag{2.8}$$

Dans ces formules, ε représente le taux de perte, q, la taille de la file d'attente et C, la capacité. Les paramètres α_{long} et α_{short} dictent un intervalle de confiance pour les contraintes. Des études ont montré que chacun peut être basé sur la valeur $Q^{-1}(\ )$ d'une

distribution normale $N(0, 1)$ [11]. La largeur de bande à l'échelle de temps de la rafale est liée à la taille du tampon, et la valeur de la capacité du lien est requise pour déduire le taux auquel le tampon peut être saturé. Il faut remarquer que l'estimé à long terme ne considère qu'une seule échelle de temps (la plus grande) par opposition à l'estimé à court terme qui examine toutes les échelles de temps I_η identifiées dans le but de trouver l'estimé le plus pessimiste. À l'aide des valeurs E_{long} et E_{short}, la largeur de bande effective finale est dérivée [3]:

$$E = \max\{E_{long}, E_{short}\}$$

Ensuite, l'algorithme construit pour la requête une enveloppe de trafic R_k^β en se basant sur son taux maximal déclaré p (*peak rate*), l'échelle k et la période élémentaire [3]:

$$R_k^\beta = \frac{p}{k \times \tau}$$

En conséquence, le processus de décision est segmenté en deux composantes : la première est associée à la dynamique du tampon et l'autre, à ses fluctuations à long terme. Il considère donc la capacité B du tampon et la capacité C du lien. Le critère de décision basé sur le seuil *P-TO* vérifie si les inéquations suivantes sont respectées [3]:

$$\max_{k=1,2,\ldots,T} \left\{k\tau\left(\overline{R_k} + R_k^\beta + \alpha_{short}\,\sigma_k - C\right)\right\} \leq B \qquad (2.9)$$

et

$$\overline{R_T} + R_T^\beta + \alpha_{long}\,\sigma_T \leq C \qquad (2.10)$$

Cela dit, le choix des paramètres de ces mécanismes est difficile pour obtenir un bon niveau de performance.

2.6.4 Considérations importantes des MBAC

Les considérations des mécanismes de contrôle d'admission basés sur les mesures sont diverses. Certaines peuvent être prises en compte plus facilement que d'autres lors du design de ces processus. Cette section nomme les éléments qui peuvent être réglés.

D'abord, le type de mesure, la taille de la période et le nombre d'échantillons sont également critiques. Si la taille de la période est trop petite, une interaction indésirable peut se produire entre le trafic et le routage. Celle-ci est mal comprise ; pourtant, elle peut conduire à un approvisionnement en ressources inadéquat (trop grand ou trop petit) ou encore à des oscillations dans les quantités offertes. Plus le nombre d'échantillons est élevé, plus les estimés risquent d'être corrects. Ensuite, il existe une interaction entre la structure de corrélation du trafic et la dynamique des départs et entrées des flots dans le système. En outre, l'impact des décisions erronées d'admission sur le mécanisme MBAC est non négligeable contrairement à ce que supposent implicitement plusieurs mécanismes de contrôle d'admission basés sur des mesures (l'hypothèse que l'effet à long terme est négligeable est remis en doute, entre autres, parce que la probabilité d'accepter par erreur un flot n'est pas égale à celle de le rejeter). Par ailleurs, un point important pour le système d'ingénierie de trafic est le délai de communication des mesures entre leur point d'acquisition et l'estimateur. Ensuite, il faudrait éviter certaines hypothèses, notamment celles concernant l'homogénéité du trafic et les propriétés stochastiques simplifiées du trafic. Enfin, plusieurs études ont soulevé la difficulté de prédire la performance des MBAC et, par conséquent, de déterminer un choix de valeurs pour les paramètres réglables qui donne lieu à un niveau de performance donné [11].

Cela dit, il n'existe pas de module parfait. Aussi, pour le design d'un mécanisme de contrôle d'admission, il convient de déterminer les éléments prioritaires dans une situation donnée et de les privilégier (en faisant évidemment un effort de compromis global). De manière générale, il est souhaitable que le mécanisme soit simple, précis,

stable, évolutif, rapide et flexible. Enfin, il ne devrait pas engendrer un surcroît de signalisation dans le réseau.

2.6.5 Mise en contexte pour UMTS

Dans le domaine à commutation de paquets du réseau de cœur, deux modules de contrôle d'admission fournissent une décision partielle pour répondre aux requêtes d'activation et de modification de contexte PDP. Ils sont logés dans le SGSN et le GGSN. En faisant abstraction du volet « politique », il est possible de résumer le deuxième volet. Sur réception d'une requête sur la liaison montante, le SGSN exécute localement un algorithme de contrôle d'admission, puis envoie au GGSN une requête *Create PDP Context*. Ce dernier exécute localement un algorithme de contrôle d'admission basé sur des politiques, puis transmet sa réponse, positive ou négative, au SGSN. Celui-ci détermine la réponse finale à l'aide des décisions de l'UTRAN et du réseau cœur et l'achemine à l'usager. Aussi, afin d'accepter autant de requêtes que possible, il faut optimiser la composante « disponibilité des ressources » du mécanisme de contrôle d'admission basé sur des politiques.

2.7 Problèmes ouverts

À la lumière de cette revue de littérature, une liste exhaustive de problèmes ouverts peut être dressée. Cette section mentionne quelques cas non résolus.

D'emblée, le domaine à commutation de paquets ne dispose pas d'un mécanisme de contrôle d'admission qui s'appuie sur des politiques et sur la disponibilité globale des ressources. Le surdimensionnement et le conditionnement sont préconisés. Le SGSN n'est pas un client de politiques et son module d'admission est spécifique à l'opérateur/vendeur. Le mécanisme du GGSN est le seul à être basé sur des politiques.

Ensuite, l'indexation des politiques à l'aide des paramètres de l'application SDP est immature, de même que la mise en correspondance des paramètres SDP avec ceux de la QdS IP. De surcroît, le modèle d'information des politiques peut être amélioré. Le

contenu des politiques des services doit être clairement défini, de même que les mécanismes pour leur enregistrement et leur retrait. Par ailleurs, des mécanismes doivent être définis pour l'enregistrement et le retrait des mesures. Celles-ci devraient être conservées dans un nœud central et extraites de manière cohérente. Une relation étroite doit aussi être conservée entre les mécanismes de politiques et les mesures d'ingénierie de trafic, car le contenu des politiques risque d'être obtenu à partir des applications d'ingénierie de trafic.

En outre, il faut définir le contrôle des ressources de QdS pour les applications SIP et non-SIP. Enfin, l'agrégation des priorités dans un routeur pose un problème, car elle est effectuée en même temps que l'agrégation des réservations ; or celles-ci peuvent être hétérogènes (différents flowspecs par exemple).

La norme UMTS étant en cours de normalisation, plusieurs éléments ne sont pas explicités. Ceci a pour effet d'alimenter la recherche.

CHAPITRE 3
SCHÉMA DE GESTION ET MÉCANISME DE CONTRÔLE D'ADMISSION BASÉS SUR DES POLITIQUES

Dans ce mémoire, nous proposons un schéma de fonctionnement basé sur des politiques. Nous suggérons aussi un algorithme qui est tiré de la littérature pour réaliser l'application d'ingénierie de trafic qui est souhaitée. Il s'agit de montrer comment il est possible d'enrichir la gestion basée sur des politiques avec la connaissance de la disponibilité des ressources. Les pièces de la solution finale sont liées aux volets « politique » et « disponibilité des ressources » et sont puisées, essentiellement, de documents qui portent sur la gestion basée sur des politiques ou sur les mécanismes de contrôle d'admission basés sur des mesures. Dans ce chapitre, les schémas de fonctionnement envisagés sont d'abord décrits. Les extensions employées par ces derniers sont par la suite présentées. Finalement, après avoir précisé les modules de contrôle d'admission choisis, les scénarios sont analysés pour dégager la solution retenue.

3.1 Description des schémas de fonctionnement basés sur des politiques

Les scénarios proposés formulent les objectifs des systèmes d'ingénierie de trafic, c'est-à-dire l'utilisation efficiente des ressources finies du réseau et le respect, dans la mesure du possible, des exigences en QdS qui sont intrinsèques aux applications. Dans cette section, le sous-système dédié aux services IP élaborés est d'abord expliqué. Ensuite, les schémas sont comparés les uns avec les autres. Les explications ci-après données mettent l'accent sur la contribution de la connaissance de l'utilisation des ressources à la gestion basée sur des politiques.

3.1.1 Sous-système dédié aux services IP élaborés et ingénierie de trafic

Dans le cadre générique de 3GPP, l'approche de gestion basée sur les politiques des services se fonde sur le sous-système multimédia IMS. Elle concerne donc exclusivement les applications multimédias. Il s'ensuit que le type de traitement accordé à un flot est basé sur sa classe de QdS. Or, un niveau de QdS peut être influencé par une variété de facteurs, tels la nature de l'application et le groupe d'appartenance de l'usager. Cette constatation motive notre proposition d'un sous-système pour les services de QdS IP élaborés ainsi que l'emploi des technologies MPLS et DiffServ pour l'ingénierie de trafic. Le sous-système remplace le module IMS et est dénommé *Enhanced IP Services Subsystem* (EISS). Cette section explique les choix.

En vue d'offrir des niveaux de QdS en fonction d'une variété de facteurs, les schémas de fonctionnement imaginés utilisent le sous-système EISS. Les niveaux sont indiqués dans la base de l'opérateur pour les profils des abonnés et sont largement influencés par la grille de tarification. Ainsi, un usager de la défense nationale, du gouvernement ou encore d'une compagnie très lucrative, par exemple, peut souscrire à un niveau de QdS élevé, moyennant, cependant, des frais non négligeables. Les services IP non élaborés reçoivent le traitement classique. En outre, pour des fins d'ingénierie de trafic, nous employons les technologies MPLS et DiffServ [25, 26, 27, 28]. Cette combinaison allie les avantages des deux méthodes et pallie certains de leurs inconvénients. En effet, MPLS effectue la répartition logique du trafic à travers le réseau dans le but de combattre la congestion de manière proactive (LSP explicites, de pis-aller, etc.). En revanche, DiffServ réalise une allocation des ressources entre les agrégats de flots concurrents en se basant sur le critère de classe. Plus précisément, il traite les paquets en se fondant sur la valeur *Per-hop Behavior PHB* de l'agrégat, laquelle est déterminée par la valeur du champ *DiffServ CodePoint DSCP* de l'entête IP du paquet. Cet objet étant de six bits, il spécifie une borne de soixante-quatre pour le nombre de niveaux de QdS. L'opérateur définira autant de classes que de niveaux de QdS souhaités et supportés. Présentement, dans DiffServ, les niveaux de QdS sont EF,

AFxy et BE, avec x, le numéro de classe allant de un à quatre et y, la probabilité de rejet allant de un à trois. AFxy spécifie douze PHB.

Dans nos solutions, les deux technologies réalisent l'ingénierie de trafic à l'aide de E-LSP dynamiques ou de L-LSP pseudo-statiques. Chaque FEC possède un LSP primaire et des LSP secondaires et est entièrement décrit avec les adresses source et destination et la classe de QdS. Nous employons des LSP de type L-LSP parce qu'ils permettent de définir jusqu'à soixante-quatre niveaux de QdS, ce que ne permet pas de faire son concurrent E-LSP dont le nombre de combinaisons possibles est limité par le champ EXP de l'en-tête MPLS (huit classes par LSP). Entre parenthèses, le qualificatif « pseudo-statique » pour les LSP est expliqué plus tard.

3.1.2 Schéma fondé sur des E-LSP dynamiques

Ce schéma de fonctionnement repose sur les technologies MPLS, DiffServ et SNMP. Les deux premières technologies réalisent l'ingénierie de trafic à l'aide de E-LSP dynamiques. Le standard SNMP est employé pour acquérir les mesures d'utilisation des interfaces par classe. Ensuite, le SGSN intègre un point de renforcement des politiques de sorte qu'il adopte un comportement similaire à son proche GGSN. Il le dispense donc de la gestion des requêtes sur la liaison montante. De plus, chaque nœud GSN exécute un mécanisme de contrôle d'admission sur réception d'un message lié à une requête d'activation ou de modification de contexte PDP. Cet algorithme vérifie essentiellement la disponibilité des mesures sur les interfaces. Le niveau de décision est donc semi-distribué. Ce scénario emploie une extension SNMP pour les mesures et les identifiants des interfaces. Le schéma est illustré à la Figure 3.1 pour une requête acceptée (sans le message COPS-Rpt donnant le résultat de l'exécution de la décision). Certaines procédures ne sont pas montrées pour des fins de clarté.

Pour illustrer ce schéma de fonctionnement, prenons le cas d'une requête unidirectionnelle sur la liaison montante. Sur réception de cette requête, le SGSN extrait de ses bases MIB les niveaux de charge des interfaces, puis exécute un mécanisme

MBAC en se basant sur les mesures fournies. Les interactions COPS pour le volet « politique » se produisent ensuite avec le PCF.

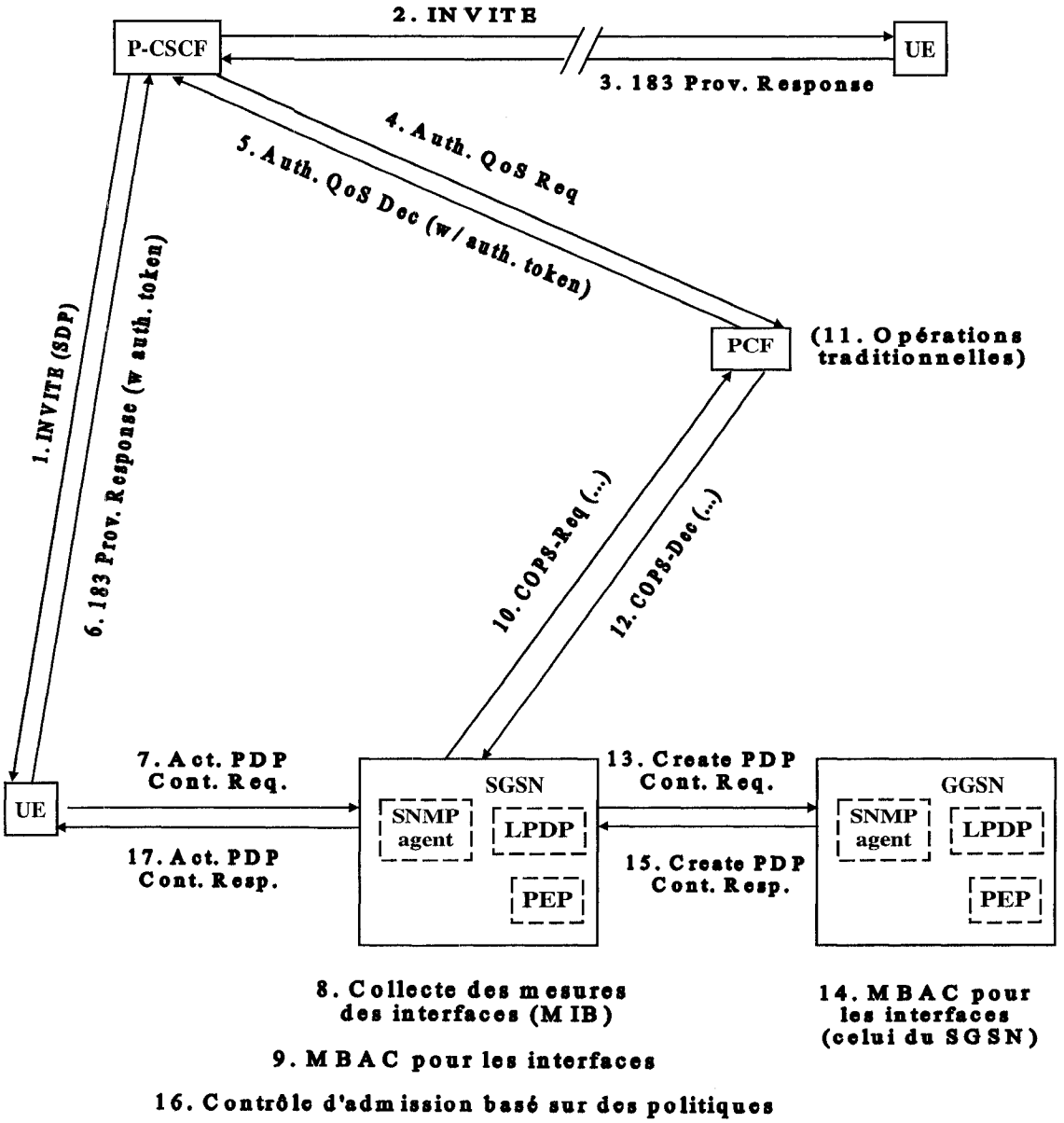

Figure 3.1 Schéma fondé sur des E-LSP dynamiques et un MBAC basé sur les mesures des interfaces

Cependant, avant d'attendre la réponse du PCF, le SGSN envoie une requête de création de contexte PDP au GGSN. Ce dernier indexe les niveaux de charge des interfaces qui sont conservés dans sa base MIB et exécute le mécanisme de contrôle d'admission basé sur des mesures. Les nœuds GSN implémentent le même algorithme MBAC et font d'autres vérifications (celles de 3GPP). La suite des opérations est celle prévue par 3GPP. Fait important à noter, ce schéma s'apparente au cadre générique de 3GPP, excepté l'intégration du PEP au SGSN et les autres modifications mineures.

3.1.3 Schémas de fonctionnement apportant un degré de complexification au cadre générique de 3GPP

Les schémas subséquents font usage de mécanismes de QdS nettement plus élaborés que le précédent. Ils sont regroupés dans cette sous-section parce qu'ils essaient de mieux composer avec les exigences de QdS posées par les applications. Il apparaît donc nécessaire de motiver la complexification au cadre générique de 3GPP que nous introduisons et de la justifier face au premier schéma. Cette sous-section donne les raisons en faveur des modifications apportées qui peuvent sembler à première vue discutables.

Comme expliqué au chapitre deux, le module de contrôle d'admission basé sur des politiques doit reposer sur des mesures s'il veut parvenir à combattre efficacement la congestion. Dans le but de fournir des décisions conséquentes, il doit s'appuyer sur des données représentatives de la disponibilité des ressources dans le domaine à commutation de paquets du réseau de cœur. Pour obtenir les mesures et les relayer au mécanisme de contrôle d'admission, le processus d'acquisition des mesures peut reposer sur les messages de largeur de bande résiduelle par classe qui sont échangés entre les routeurs ou encore prélever les mesures sur des chemins déjà établis, par exemple, sur des LSP. Nous optons pour la méthode qui consiste à collecter les données sur des LSP, malgré les vertus de l'autre candidate. Elle implique l'emploi de LSP établis à l'avance. Les schémas subséquents sont fondés sur cette méthode.

Ensuite, dans le cadre générique de l'IETF, le serveur de politiques PDP peut être placé dans un *Bandwidth Broker*, une entité, par définition, tenue de connaître la topologie de son domaine et la disponibilité des ressources globales [29]. À titre de rappel, ce concept de l'IETF est associé aux réseaux DiffServ, lesquels – nous le savons - relèguent les tâches complexes de classification et de conditionnement aux nœuds frontières du domaine et dispensent, à toutes fins pratiques, les nœuds intermédiaires des fonctions élaborées. Il apparaît donc naturel que les mesures sur les L-LSP soient prélevées par les GSN, car ils se trouvent en périphérie du domaine. À l'aide des technologies MPLS et DiffServ (des L-LSP), un processus efficace d'acquisition des mesures peut être conçu, c'est-à-dire avec des indicateurs de niveau d'utilisation des ressources globaux et par classe. Ce sont ces considérations qui ont motivé l'emploi des mécanismes des prochains schémas [34].

3.1.4 Schémas de fonctionnement fondés sur des L-LSP pseudo-statiques

Ces scénarios sont manifestement plus soucieux de respecter le contrat de qualité de service. Leurs similarités sont multiples. Dans les lignes qui suivent, après avoir énuméré les points communs des trois schémas, nous les décrivons sommairement.

En ce qui concerne les ressemblances des scénarios, elles sont importantes. À l'aide de MPLS et de DiffServ, ceux-ci établissent et dimensionnent des L-LSP à l'avance en vue de satisfaire les exigences de QdS des agrégats de flots. Les LSP sont dits pseudo-statiques parce qu'ils sont établis généralement à l'avance, mais leur durée de vie dépasse l'échelle d'une session unique. En fait, le PCF est censé ordonner la création et la modification des LSP à moyen terme. La décision peut être imputable à des politiques événementielles ou temporelles telles que des statistiques à long terme d'utilisation des LSP, des pannes ou des moments de la journée. Le SGSN mesure périodiquement le niveau de charge des LSP sur la liaison montante et le GGSN en fait de même sur la liaison descendante. Les mesures sont conservées dans les nœuds GSN en totalité ou en partie. Par ailleurs, pendant la durée de vie d'un LSP, la base FTN est mise à jour pour discriminer les flots autorisés. Donc, si les LSP sont créés à l'avance,

ils sont remplis et vidés par les flots en fonction des départs et entrées de ceux-ci du système.

En outre, le SGSN intègre un point de renforcement des politiques de sorte qu'il adopte un comportement similaire à son proche GGSN. Il le dispense de la gestion des requêtes sur la liaison montante. Enfin, dans pratiquement tous les schémas, le serveur de politiques PCF est intégré à un *Bandwidth Broker*. Cette entité nouvelle figure dans l'architecture globale de tous les scénarios, excepté le dernier. Elle s'acquitte de la gestion globale des ressources et possède une base de données renfermant les mesures de disponibilité des ressources. En ce qui concerne les particularités des schémas, elles sont liées essentiellement au degré de décentralisation qui caractérise les processus pour l'acquisition des mesures, l'analyse et l'optimisation. Noter que les schémas utilisent une extension COPS et/ou SNMP.

- ***Schéma fondé sur un Bandwidth Broker, des messages COPS-RPT périodiques, des L-LSP pseudo-statiques et un MBAC basé sur les mesures des LSP***

Ce schéma de fonctionnement inclut un *Bandwidth Broker* qui dispose d'une connaissance globale des ressources LSP disponibles dans le domaine. Cette entité implémente le processus d'analyse proposé, c'est-à-dire le mécanisme de contrôle d'admission qui s'appuie sur les mesures des LSP pour évaluer la disponibilité des ressources. Le processus d'acquisition des mesures emploie des rapports périodiques pour collecter et transmettre les données de mesures relatives aux LSP.

Ainsi, les informations de mesures sont temporairement stockées dans les bases PIB des GSN et extraites périodiquement pour être communiquées au BB (PCF) via des messages de type COPS-RPT. La base de données du PCF contient la totalité des mesures, par opposition aux bases PIB des GSN qui ne renferment qu'un nombre limité de données instantanées. La fréquence des rapports est déterminée par la valeur de l'objet *AccTimer*. Il revient au BB (PCF) d'implémenter le mécanisme de contrôle d'admission basé sur des mesures et de l'exécuter sur réception d'une requête COPS liée à un message d'activation ou de modification de contexte PDP. La décision que le PCF

transmet au PEP du GSN renferme l'identifiant du LSP disponible. Si aucun LSP n'est trouvé ou si un problème est détecté, la décision précise plutôt une valeur nulle et un code d'erreur.

À la Figure 3.2, les procédures sont illustrées pour une requête unidirectionnelle qui est acceptée sur la liaison montante (sans le message COPS-Rpt donnant le résultat de l'exécution de la décision). Sur réception d'un message d'activation/de modification de contexte PDP, le SGSN envoie au BB (PCF) un message COPS-Req qui renferme les données classiques (jeton d'autorisation, et autres). Le serveur de politiques indexe de sa base PIB les mesures des LSP de la classe de la requête, puis exécute l'algorithme MBAC. Il fait aussi les opérations liées aux politiques. Le PCF achemine par la suite au SGSN un message COPS-Dec qui renferme l'identifiant du LSP disponible, le cas échéant une valeur nulle avec un code d'erreur. Après, le SGSN effectue les opérations prévues par 3GPP pour un PEP (mise en correspondance, comparaison), puis transmet au GGSN la requête de création de contexte PDP. Le nœud passerelle fait les vérifications prévues par 3GPP (limite sur le nombre de contextes PDP, etc.) et véhicule sa réponse au SGSN. La suite des procédures est celle prévue dans 3GPP (avec l'UTRAN et l'usager). Les opérations sont semblables pour une requête sur la liaison descendante, excepté que c'est le GGSN qui envoie la requête COPS.

Une extension COPS est requise pour spécifier les mesures et les identifiants des LSP ainsi que les éléments de la table FTN.

- ***Schéma fondé sur un Bandwidth Broker, des L-LSP pseudo-statiques, des échanges SNMP périodiques et un MBAC basé sur les mesures des LSP***

Ce scénario inclut un *Bandwidth Broker* dont la connaissance des ressources LSP disponibles est globale, mais morcelée dans le temps. Le MBAC constitue le processus d'analyse proposé. Il est alimenté des données des LSP et logé dans le nœud central BB. Quant au processus d'acquisition des mesures, il a recours à SNMP pour sauvegarder et communiquer les données relatives aux LSP. Dans ce schéma, le BB (PCF) comprend une entité manager. Chaque GSN contient une entité agent qui acquiert périodiquement

les mesures et les stocke dans une base MIB interne. Ces données sont régulièrement sollicitées par le manager du BB (PCF), puis conservées dans sa base MIB.

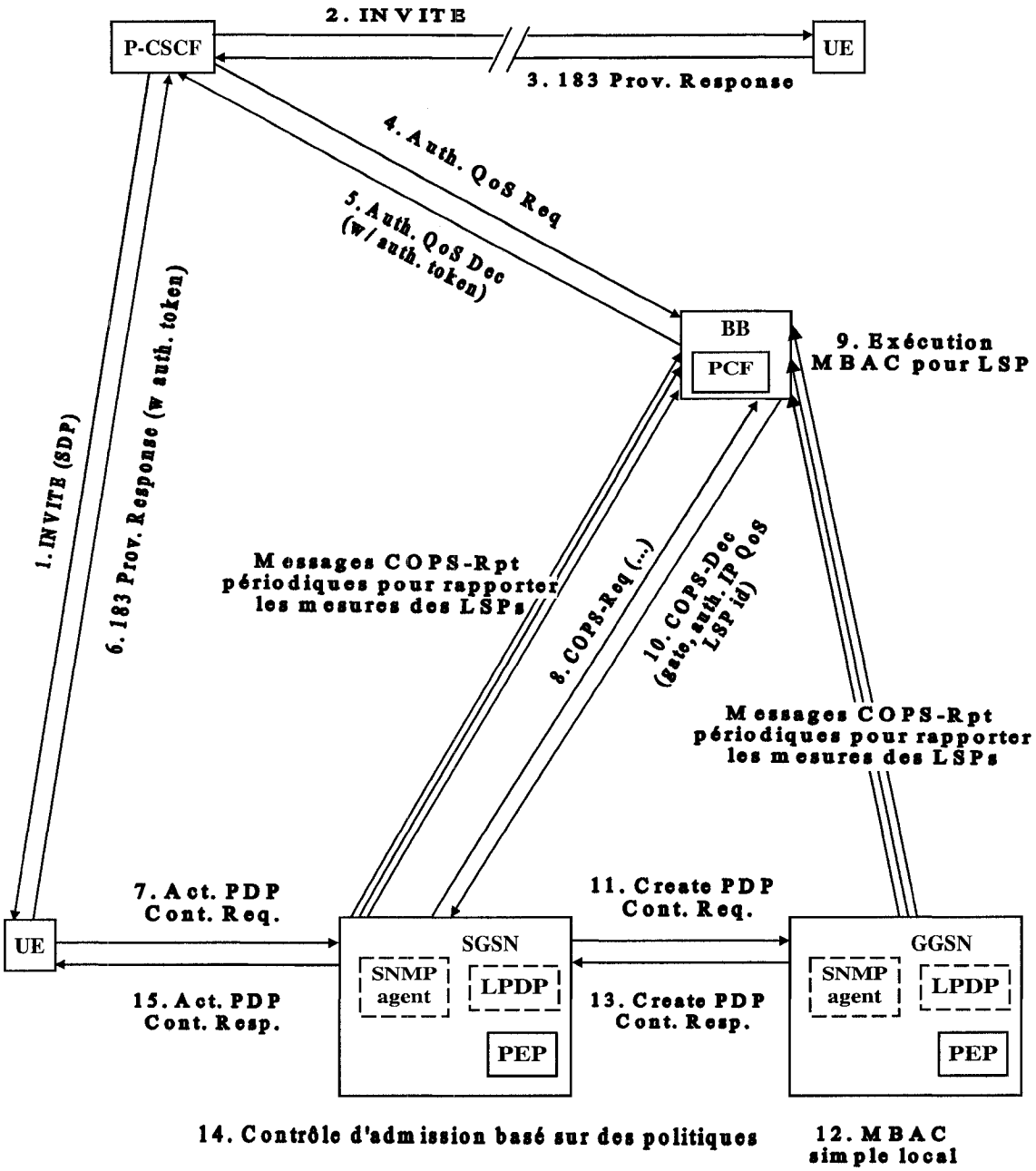

Figure 3.2 Schéma fondé sur un *Bandwidth Broker*, des messages COPS-RPT périodiques, des L-LSP pseudo-statiques et un MBAC basé sur les mesures des LSP

Ce scénario définit une extension COPS qui spécifie les identifiants des LSP et les éléments de la table FTN. Il utilise aussi une extension SNMP qui précise les mesures et les identifiants des LSP. Entre parenthèses, deux nœuds externes disposant d'un grand espace mémoire peuvent être ajoutés à l'architecture, l'un pour le SGSN et l'autre pour le GGSN. Ils peuvent incorporer un *manager* et un agent pour communiquer respectivement avec l'agent du GSN et le *manager* du BB (PCF).

À titre d'exemple, sur réception d'une requête d'activation de contexte PDP, le SGSN envoie au BB (PCF) un message COPS-Req qui renferme les informations classiques. Le *manager* du BB (PCF) indexe les mesures récentes des niveaux de charge qui se rapportent aux LSP de la classe de la requête. Ces mesures lui sont nécessaires pour exécuter le MBAC. La suite des procédures est semblable à celle du schéma précédent. Si des nœuds externes sont employés, un message *getBulkRequest* est acheminé à l'agent du nœud GSN pour obtenir les mesures. La Figure 3.3 illustre une requête acceptée sur la liaison montante. Les messages COPS-Rpt donnant le résultat de l'exécution de la décision ne sont pas montrés. Cela dit, quelques modifications à ce schéma permettent de définir un scénario supplémentaire, soit la solution alternative de ce schéma.

Solution alternative

Dans cette solution, les mesures sont demandées par le BB sur réception d'une requête d'activation ou de modification de contexte PDP.

- ***Schéma fondé sur des serveurs LPDP, des L-LSP pseudo-statiques, des données SNMP et un MBAC basé sur les mesures des LSP***

À l'instar du précédent scénario, le processus d'acquisition des mesures de ce schéma a recours à SNMP pour sauvegarder et acheminer les données des LSP. Cependant, un *Bandwidth Broker* n'apparaît pas dans l'architecture du système.

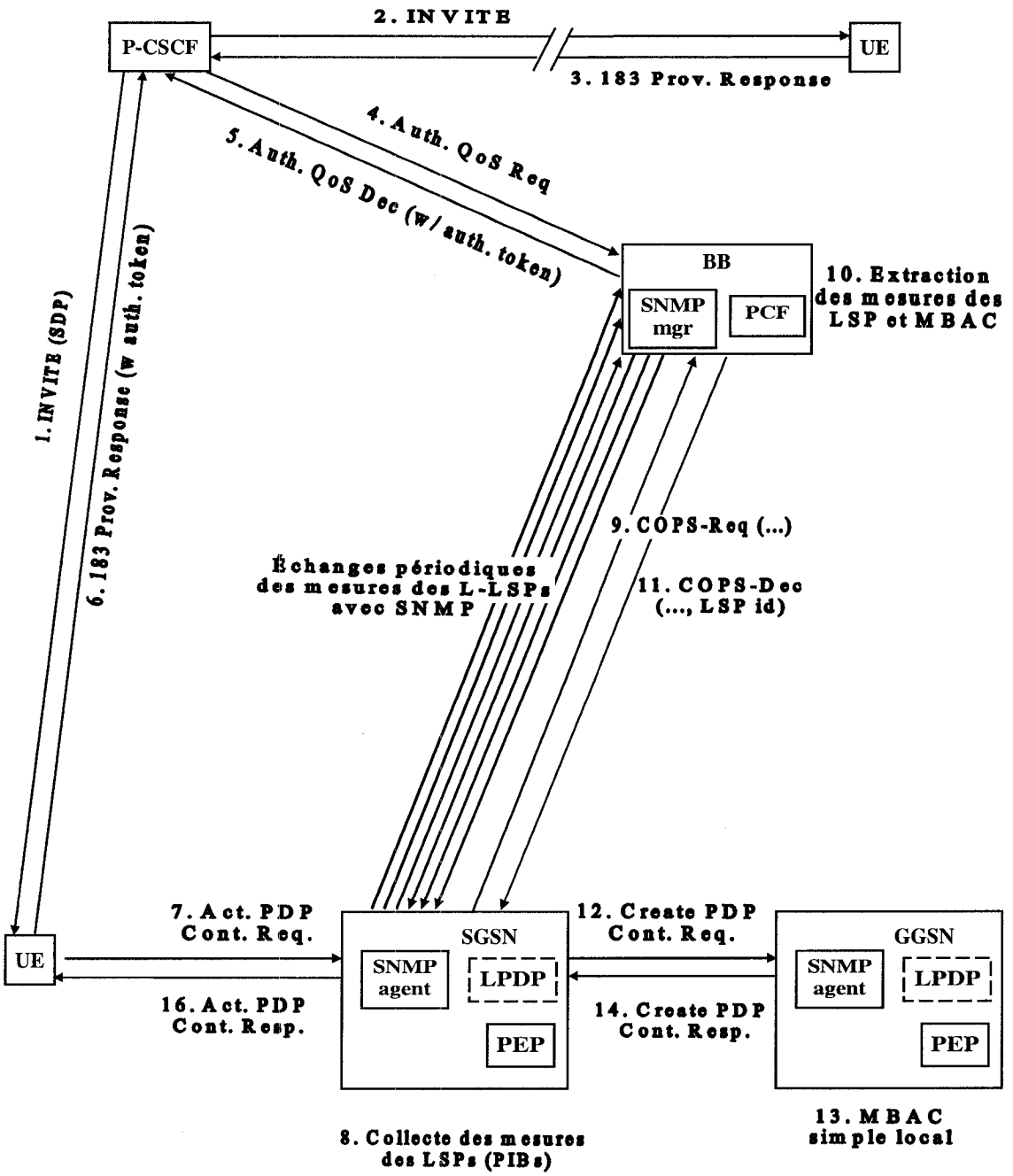

Figure 3.3 Schéma fondé sur un *Bandwidth Broker*, des L-LSP pseudo-statiques, des échanges SNMP périodiques et un MBAC basé sur les mesures des LSP

Ainsi, les mesures des niveaux de charge des LSP ne sont pas véhiculées à un processus externe pour les fins visées par le contrôle d'admission basé sur des mesures. Ce scénario impute aux serveurs de politiques LPDP des nœuds GSN la responsabilité de fournir une décision relativement à la disponibilité des ressources LSP. La collecte des mesures et l'analyse MBAC sont réalisées dans les GSN. La réponse du serveur LPDP révèle la décision du MBAC. Elle est communiquée au client de politiques, puis véhiculée par ce dernier au serveur PCF dans un message COPS-Req. La décision locale et les informations traditionnelles sont considérées par le PCF pour formuler une décision cohérente avec les politiques de l'opérateur et la disponibilité des ressources dans le domaine. La Figure 3.4 illustre un cas de requête acceptée (sans COPS-Rpt).

Par exemple, sur réception d'une requête d'activation ou de modification de contexte PDP sur la liaison montante, le PEP du SGSN envoie au serveur LPDP un message COPS-Req qui renferme les informations traditionnelles. Le LPDP demande à l'entité agent les données liées aux LSP de la classe de la requête. Lorsque les informations sont connues, le SGSN exécute l'algorithme MBAC basé sur les mesures des LSP. Ensuite, le serveur LPDP envoie au PEP une décision qui indique l'identifiant du LSP disponible ou une valeur nulle. Le SGSN insère ces données et les informations classiques dans un message COPS-Req, puis les transmet au PCF. Le serveur central considère l'ensemble des informations fournies pour déterminer sa décision. Les opérations sont semblables pour une requête sur la liaison descendante. Ce scénario définit une extension COPS qui spécifie les identifiants des LSP et les éléments de la table FTN. Il utilise aussi une extension SNMP qui précise les mesures et les identifiants des LSP. Le PCF utilise les modules prévus par 3GPP.

Dans les quatre scénarios, si une requête d'activation ou de modification de contexte bidirectionnelle est reçue, la disponibilité des ressources est vérifiée sur les liaisons montante et descendante. Les deux GSN adoptent un comportement similaire. Pour accepter la requête, deux LSP doivent être trouvés. Dans le deuxième schéma, le troisième et sa solution alternative, le BB s'acquitte d'obtenir les données de mesures sur les deux liaisons. Dans le dernier, les GSN exécutent le même processus d'analyse.

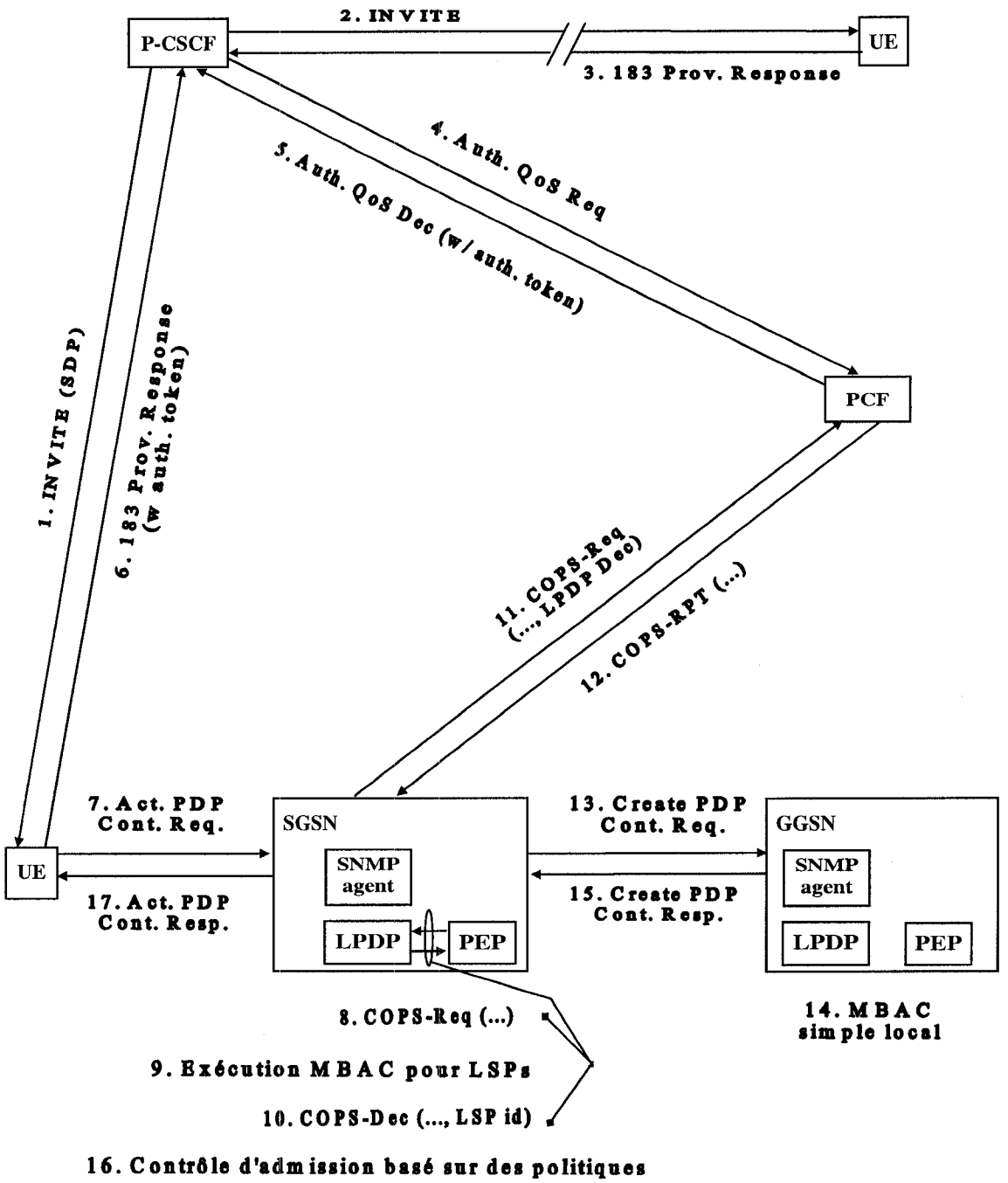

Figure 3.4 Schéma fondé sur des serveurs LPDP, des L-LSP pseudo-statiques, des données SNMP et un MBAC basé sur les mesures des LSP

Noter que l'emploi par les schémas d'un serveur LPDP dans les nœuds GSN leur confère une certaine tolérance aux pannes. Entre parenthèses, les requêtes qui conduisent à des interactions entre les nœuds de politiques sont celles qui sollicitent un niveau de QdS élevé. Le sous-système multimédia devient donc un sous-système qui œuvre pour les connexions associées à des niveaux de QdS élevés.

3.2 Extensions possibles pour COPS et SNMP

Les extensions référées par les schémas de fonctionnement s'appliquent à COPS et à SNMP. Les règles précisées par l'IETF doivent être prises en compte, notamment pour assurer la compatibilité avec les anciennes versions des modules. Deux types d'extensions sont nécessaires pour COPS et deux le sont pour SNMP. Les nouvelles classes PRC de COPS peuvent être véhiculées dans les objets de type Client-SI et/ou de type *Named Decision Data*. Elles indiquent les mesures et les identifiants des LSP ou des interfaces. Les objets nouveaux de SNMP sont transportés dans les messages échangés entre les entités concernées. Les formats des messages COPS et SNMP ne sont pas changés. Cette section traite des extensions.

3.2.1 Modifications liées à COPS

Afin de conserver dans des bases PIB les informations relatives aux LSP ou aux interfaces et afin de les convoyer entre les nœuds de gestion des politiques, nous prévoyons deux types d'extensions COPS. Avant toute chose, il importe de mentionner que l'en-tête commun des messages COPS doit préciser un nouveau type de client. Cette valeur, qui est insérée dans le champ Client-type, donne le cadre d'interprétation conséquent pour les messages spécifiques au client. Le numéro doit être assigné par l'IANA.

Dans les différents schémas, les messages COPS-Req/COPS-RPT et COPS-Dec comprennent de nouvelles classes PRC pour les fins visées de gestion et de contrôle d'admission basé sur des politiques. Le premier type d'extension est employé par les

scénarios deux et quatre et le second, par le troisième et sa solution alternative. La première extension indique l'identifiant du LSP, ses niveaux de charge récents ainsi que les éléments FEC et NHLFE de la table FTN. La seconde extension définit les identifiants des LSP et les éléments FEC et NHLFE de la table FTN. En plus de spécifier ces classes, nous pouvons nous attendre à ce que les extensions précisent des PRC supplémentaires telles les propriétés des LSP, des variables d'état, et autres.

Pour définir ces extensions, les modules existants peuvent être employés, moyennant des modifications mineures ou majeures. Par exemple, le module MPLS TE PIB peut constituer un bon point de départ [30] pour les scénarios, le premier excepté. Il a été élaboré pour permettre l'établissement des tunnels MPLS à l'aide de RSVP-TE et pour réaliser l'affectation du trafic entrant à un LSP avec DiffServ et MPLS. Les tables *FECTable* et *LSPTunnelTable* sont particulièrement intéressantes pour nos extensions, mais des attributs doivent leur être ajoutés et d'autres tables sont nécessaires. Pour le scénario fondé sur les rapports périodiques COPS-Rpt, il est possible de se servir du module *IP TE Accounting PIB* moyennant certaines modifications [31]. Cependant, le module de classes PRC qu'il inclut pour les mesures d'utilisation des LSP (*LspTEAccountingClasses*) est vide et devrait être défini. Ce module constitue une extension d'un module PIB global rédigé pour l'ingénierie de trafic [30, 32]. Dans tous les cas, il est possible de concevoir un module PIB intégralement et d'importer les définitions nécessaires de modules PIB ou MIB extérieurs, particulièrement pour une extension simple comme la première. À titre indicatif, les changements aux modules PIB autorisés sont néanmoins limités : de nouvelles PRC peuvent être ajoutées à une table PIB ou supprimées de celle-ci, des attributs peuvent être ajoutés ou supprimés d'une classe PRC existante et, finalement, une classe PRC existante peut être augmentée d'une classe PRC tirée d'un autre module PIB.

En outre, afin d'enrichir la gestion basée sur des politiques, il serait intéressant de concevoir une série de modules PIB et de les utiliser. En effet, il est souhaitable de pouvoir exécuter une variété d'actions de politiques. Citons, à titre d'exemple, les politiques qui définissent l'hybride de statisme et de dynamisme lié aux L-LSP. Cette

ambivalence est due aux politiques et caractérise les schémas deux et trois ainsi que sa solution alternative. À titre de rappel, le serveur PCF commande à l'occasion - à moyen terme - la fermeture des L-LSP activés, leur modification et la création de L-LSP nouveaux avec des propriétés bien définies. La création, la modification et la fermeture dynamique sont effectuées avec RSVP-TE (RESV-TEAR, etc.). Les décisions asynchrones du PCF peuvent découler de l'activation d'une politique particulière existante ou être imputables à une mise à jour du contenu de la centrale de dépôt par la console. Par exemple, une politique peut demander de fermer des LSP et d'en établir d'autres à certains moments de la journée, changer la valeur d'un paramètre donné d'un module d'ordonnancement en fonction de mesures d'utilisation ou changer la valeur d'une variable d'état pour ordonner au PEP de basculer vers un mode de fonctionnement palliatif (advenant un événement particulier, tel une attaque de déni de service ou une panne). Les mises à jour des politiques peuvent s'imposer lorsque des statistiques d'utilisation des ressources à long terme sont rendues disponibles (points persistants de congestion, patrons d'utilisation, etc.). Toutefois, l'élaboration des conditions et des actions de politiques commande un effort humain appréciable.

3.2.2 Modifications liées à SNMP

Pour alimenter le sous-système d'analyse, le processus d'acquisition des mesures peut s'appuyer sur une des deux extensions SNMP. Elles sont expliquées dans les lignes qui suivent.

Dans les schémas basés sur SNMP, les objets MIB supplémentaires précisent les identifiants et les mesures des LSP. Ces informations se rapportent à des interfaces dans le premier scénario et à des LSP dans les autres schémas. Il est possible de dériver à partir de modules MIB déjà définis l'extension de chaque scénario. Les définitions spécifiées dans des bases externes peuvent aussi être ré-utilisées. Par exemple, le module MPLS TE MIB peut constituer un bon point de départ [30]. Citons la table *mplsTunnelPerfTable* et la table *mplsTunnel* qui augmente la première. Leur base MIB est associée à d'autres bases MIB MPLS - FTN, LSR, et autres - qui peuvent être

nécessaires pour la description complète du module ou facultatives. Une fois de plus, l'emploi de modules SNMP supplémentaires peut enrichir la gestion des ressources.

Pour ainsi dire, afin de donner lieu à une gestion réellement automatisée du réseau, il serait intéressant d'employer, moyennant les modifications nécessaires, les modules MIB et PIB trouvés dans la littérature. En effet, plusieurs PIB ont été définis pour répondre aux besoins de configuration et de gestion des réseaux en matière d'ingénierie de trafic, de qualité de service, de sécurité, et autres. Citons, à titre d'exemple, les modules des drafts ou des rfc qui ont été élaborés pour la sécurité, le rapport de données et les technologies MPLS, DiffServ [30, 31, 32, 33]. Il en existe au moins autant pour les MIB. De manière générale, une combinaison adéquate de modules COPS et SNMP peut automatiser une multitude d'applications d'ingénierie de trafic.

3.3 Mécanismes de contrôle d'admission basés sur des mesures

Dans le but d'évaluer la disponibilité des ressources dans le domaine à commutation de paquets du réseau de cœur, nous employons un de deux mécanismes de contrôle d'admission basés sur des mesures. Les modules retenus sont dénommés AC-MVEv2 et AC-KQv2 pour honorer leurs prédécesseurs AC-MVE et AC-KQ qui ont été décrits au chapitre deux. Cette section présente les deux modules envisagés.

En lieu et place des mesures des liens, les mécanismes utilisent les mesures des LSP. Les estimateurs et les critères de décision doivent donc être ajustés. Le premier algorithme proposé, soit le AC-MVEv2, est développé à partir du module AC-MVE qui combine l'estimateur *Mean-Variance E-MVE* et le critère de décision *Policy-Threshold P-TO*. À l'instar de son prédécesseur, le module AC-MVEv2 calcule la disponibilité des ressources sur une échelle de temps unique. Il repose sur un estimateur de type E-MVE. Cependant, il utilise un critère de décision double *P-TO/P-BP* qui se base sur la classe de la requête. Si celle-ci est de type non temps réel (nrt), le critère activé est *Policy-Threshold P-TO* ; si la classe est en temps réel (rt), le critère activé est *P-BP Policy*

Back-Off Period. Pour le second critère, si un flot donné est rejeté, un flot de sa classe doit quitter le système avant qu'une requête de la même classe puisse être acceptée.

Étant donné que l'algorithme considère des LSP, le seuil C dans est déterminé par la valeur de la capacité minimale des liens sur le LSP concerné. La période d'échantillonnage τ et la durée T de la fenêtre de mémoire valent, quant à elles, respectivement, quelques millisecondes et quelques secondes. Ensuite, pour un taux de perte ε précisé par l'usager, nous utilisons le résultat d'étude employé dans le module AC-KQ pour dériver la valeur du paramètre α' [3]. Ainsi, la question du choix de α est réglée. De plus, l'intervalle de confiance évolue avec les fluctuations observées dans le réseau de cette façon – ce qui n'était pas le cas lorsque la valeur α était fixe. La correction standard est toujours utilisée pour remédier à l'erreur d'échantillonnage. Le résultat d'étude en question indiquait que la formule suivante était adéquate pour dicter un intervalle de confiance sur la largeur de bande effective :

$$\alpha = Q^{-1}\left(\frac{\varepsilon\overline{R}}{\sigma}\right)$$

Quant au module AC-KQv2, il est dérivé du mécanisme AC-KQ qui combine l'estimateur *Traffic Envelope E-KQ* et le critère de décision *Policy-Threshold P-TO.* Il caractérise également le trafic sur plusieurs échelles de temps afin de capturer les fluctuations du trafic, à court terme et à long terme. Contrairement au mécanisme AC-KQ, le module AC-KQv2 envisagé utilise des LSP. Dans la formule E_{short} (2.6), le quotient q/C est déterminé par la valeur maximum des quotients associés aux liens traversés par le LSP. De plus, l'algorithme utilise le critère de décision double *P-TO/P-BP*, tout comme son module concurrent. Les valeurs B et C correspondent aux valeurs minimales sur les liens d'un LSP, avec B, la taille du tampon et C, la capacité du lien. La période d'échantillonnage τ et la durée T de la fenêtre de mémoire valent aussi, respectivement, quelques millisecondes et quelques secondes. Entre parenthèses, des seuils plus pessimistes peuvent être obtenus en multipliant B et C par des facteurs inférieurs à l'unité.

En somme, les mécanismes proposés adaptent les modules AC-MVE et AC-KQ. Les études ont montré que les modules de base étaient efficaces malgré leur hypothèse gaussienne [3]. Nos mécanismes emploient un critère de décision bivalué qui leur permet de basculer entre les modes conservateur et optimiste selon les garanties de QdS inhérentes à la classe de la requête. Quoi qu'il en soit, les modules envisagés font des compromis différents. Entre autres, le premier offre un temps de convergence sensiblement inférieur à son concurrent; celui-ci est plus précis que celui-là.

3.4 Critique des scénarios

Il appert qu'un système d'ingénierie de trafic repose sur quatre processus fondamentaux. Ceux-ci s'acquittent de la description des politiques, de l'acquisition des mesures, de la modélisation et de l'analyse et, enfin, de l'optimisation. Dans cette section, les scénarios présentés ci-haut sont analysés et comparés suivant les recommandations fonctionnelles et non fonctionnelles de l'IETF. Pour une description complète des recommandations, le lecteur peut se référer à l'Annexe A.9.

3.4.1 Comparaison des scénarios suivant les recommandations non fonctionnelles

Les recommandations non fonctionnelles de l'IETF précisent les attributs qualitatifs et les caractéristiques d'état qui se rapportent à un système d'ingénierie de trafic. Elles incluent, entre autres, le potentiel d'utilisation, l'automatisme, l'évolutivité, la stabilité, la flexibilité, la visibilité, la simplicité, l'interopérabilité et la sécurité. L'importance de chacun varie avec le contexte. Les scénarios sont ici comparés suivant ces recommandations.

Potentiel d'utilisation

Les cinq scénarios emploient les standards MPLS, DiffServ et SNMP; ce qui leur confère un certain potentiel d'utilisation. Les deux premières technologies sont préconisées pour UMTS et nous pouvons faire la conjecture que 3GPP prévoit utiliser

SNMP, car la popularité de ce standard est irrécusable. Cette hypothèse tient d'autant plus que le PDP de l'IETF est censé posséder une interface SNMP. De plus, le SGSN incorpore un point de renforcement de politiques. Cette modification majeure peut présenter quelques désavantages pour 3GPP, mais elle a pour effet de dispenser le GGSN, déjà très sollicité, des tâches de contrôle sur la liaison montante et donc d'améliorer la performance du réseau. En outre, nombreux sont les schémas faisant usage d'un *Bandwidth Broker*. Cette entité n'a pourtant pas encore atteint le stade de la maturité; toutefois, pour les besoins de notre système, il est possible de l'abstraire – les fonctionnalités du BB essentielles pour le fonctionnement peuvent être exécutées par un processus plus simple. Ensuite, les quatre derniers scénarios imposent la rédaction d'extensions COPS, un protocole encore immature. Mais, des objets spécifiques au client sont prévus par 3GPP pour les véhiculer. Enfin, l'emploi du sous-système EISS est très justifiable.

Si les opérateurs ne veulent pas grever leur système d'ingénierie de trafic de méthodes trop sophistiquées, le premier schéma est sans doute celui qui dispose du meilleur potentiel d'utilisation. En effet, il s'apparente au cadre générique de 3GPP, excepté le PEP dans le SGSN et les autres modifications mineures. Les modèles concurrents, quant à eux, sont plus éloignés du cadre de l'instance. Entre autres choses, la configuration manuelle, le dimensionnement, la gestion et la maintenance des L-LSP sont des tâches difficiles. Après le premier scénario, la solution alternative du troisième schéma peut sembler attrayante, car les interactions SNMP sont bien connues et non gourmandes en bande passante. Néanmoins, son *Bandwidth Broker* est inconscient de la réalité du réseau et, donc, non conforme à celui de l'IETF. Étant déterminée par les arrivées des requêtes, la connaissance du BB de la disponibilité des ressources devient morcelée dans le temps. Ensuite, nous optons pour le troisième scénario parce qu'il implique des interactions SNMP classiques, mais les ressources de l'interface sont consommées sur une base régulière pour acheminer les mesures prélevées.

Après, le schéma basé sur les messages COPS-Report est moins « utilisable » parce que les rapports d'utilisation des ressources COPS-Rpt sont moins matures [31,

32]. De surcroît, l'idée de conserver les mesures dans des bases PIB peut sembler singulière, de même que celle de les convoyer dans des messages COPS. Enfin, le quatrième schéma a un potentiel d'utilisation moindre parce que les processus des nœuds GSN deviennent assez complexes. Ce classement peut toutefois être remis en cause par un opérateur soucieux d'offrir des garanties de QdS. Dans ce cas, le premier schéma succède au troisième et précède le deuxième.

Automatisme

Par définition, la gestion basée sur des politiques est une approche d'automatisme. Conséquemment, les schémas disposent d'un niveau d'automatisme important et – mieux encore - supérieur à celui de 3GPP étant donné leur usage de modules PIB supplémentaires et d'un sous-système EISS non exclusif aux applications multimédias. En outre, des mécanismes autonomes non directement gouvernables par le PCF peuvent contribuer à accroître le degré d'automatisme du système. Cependant, le serveur PCF demeure l'entité décisionnelle ultime. Quoi qu'il en soit, les schémas sont à toutes fins pratiques comparables devant ce critère, à quelques différences près. Nous supposons que les processus SNMP et COPS peuvent communiquer entre eux correctement. Toutefois, le degré d'automatisme dépend des choix de l'opérateur, particulièrement des efforts qu'il consent à déployer pour formuler des politiques riches.

Évolutivité

De manière générale, le premier schéma est plus évolutif que ses concurrents basés sur des L-LSP. Dans ces derniers, au fur et à mesure que le nombre d'usagers, le volume de trafic et le nombre de nœuds augmentent, le nombre de L-LSP peut croître de manière substantielle; auquel cas, le dimensionnement, la gestion et la maintenance des L-LSP peuvent devenir complexes. Les bases MIB et PIB de ces schémas peuvent devenir très grosses et la signalisation liée au transport des mesures peut ravir les ressources des applications. Dans l'ensemble des scénarios, la consommation des ressources est susceptible d'être localisée, particulièrement en périphérie où se trouvent

les nœuds GSN chargés d'exécuter des modules complexes. Par ailleurs, il n'est pas possible de garantir qu'une action indésirable des processus d'acquisition des mesures et d'analyse ne se produira pas sur les autres processus. Le premier scénario a une évolutivité comparable à celle de 3GPP et supérieure aux quatre derniers schémas, car il consomme moins de ressources. En effet, il considère seulement des interfaces (et non des LSP) et son niveau de décision est semi-distribué. Cependant, la taille du domaine considéré est actuellement limitée et il serait plutôt improbable qu'elle augmente outre mesure.

Après le premier scénario, nous classons - et non sans peine - les autres candidats en ordre décroissant d'évolutivité. Nous élisons la solution alternative du troisième schéma, car elle consomme l'interface SNMP de façon parcimonieuse et parce qu'il est possible de faire un constat similaire pour ses processus d'acquisition des mesures et d'analyse. Ensuite, nous prenons le deuxième scénario et le troisième parce qu'ils sont plus centralisés que les scénarios précédents et donc plus gourmands en ressources précieuses. Si les nœuds externes sont utilisés dans le schéma trois, il devient plus évolutif parce que les ressources consommées très régulièrement sont situées au bas de l'architecture. Il faut noter que les schémas susmentionnés sont placés avant le quatrième malgré leur emploi d'un BB. Ils sont ainsi classés parce que la perte d'évolutivité de chacun avec le BB est sans doute comparable à celle de l'IETF. Enfin, le quatrième schéma est le moins évolutif de tous en dépit de son architecture semi-distribuée, car les mises à jour des politiques de la centrale de dépôt du serveur LPDP peuvent entraîner un volume important de trafic de signalisation, la fréquence de celles-ci devant être raisonnable pour assurer une certaine flexibilité au système. Dans les autres scénarios, ces mises à jour engendrent moins de trafic sur l'interface Go, car les modifications sont communiquées par la console de politiques à la centrale de dépôt. Cependant, ceci dépend de la fréquence des mises à jour. Par ailleurs, dans la quatrième solution, les nœuds GSN requièrent des ressources matérielles et logicielles coûteuses non prévues par l'instance. Les requêtes bidirectionnelles compliquent les opérations.

Stabilité

La stabilité des scénarios est surtout affectée par la période de mesure, le nombre d'échantillons, la structure de corrélation du trafic et la dynamique des départs et entrées des flots du système global. Les messages de signalisation des mesures, selon leur fréquence, peuvent apporter un surcroît d'instabilité au système d'ingénierie de trafic. De manière générale, chaque processus peut potentiellement dégrader la stabilité. Comme les cinq scénarios emploient le même algorithme d'admission, la performance de ce module ne permet pas de les distinguer. Nous pouvons toutefois dire que le mécanisme AC-KQ effectue une caractérisation du trafic sur plusieurs échelles de temps de sorte qu'il peut sans doute émettre des décisions erronées moins souvent que son concurrent AC-MVE. Dans les lignes qui suivent, nous examinons, pour chaque scénario, la stabilité des processus qui sont dédiés à l'acquisition des mesures, à l'analyse et à l'optimisation. Pour ce faire, nous employons les indicateurs de stabilité suivants de la littérature [35]: la fiabilité des nœuds, le degré de protection des liens, la fréquence des interruptions de service dues à des opérations planifiées et, enfin, le temps de convergence.

Dans l'ensemble des scénarios, les GSN et le *Bandwidth Broker* sont robustes. De plus, le BB, les GSN et les nœuds SNMP externes disposent de nœuds de backup. Les LSP ont aussi des LSP alternatifs. De manière générale, nous employons les méthodes classiques de survivabilité et de tolérance aux pannes qui sont envisagées par 3GPP ou qui sont inhérentes aux technologies déployées. Ceci a pour effet de réduire la probabilité de pannes. Citons, à titre d'exemple, la validation de la connexion, les décisions cachées du serveur LPDP et les techniques MPLS de protection et de restauration. En outre, l'emploi des modules PIB additionnels par les cinq schémas diminue le nombre d'interruptions de service planifiées, car la console de politiques peut modifier le serveur de politiques et celui-ci peut à son tour apporter des changements au client PEP sans que la connexion n'ait à être coupée. Ceci peut toutefois donner lieu à un accroissement du nombre de pannes logicielles. Ensuite, dans les quatre derniers scénarios, les tables de LSP de « lookup » participent généralement à la réduction du

temps de convergence. De plus, le contrôle exercé par le PCF pour modifier les LSP peut améliorer la stabilité si la fréquence des décisions asynchrones est raisonnable. Ces quatre schémas disposent aussi d'un mécanisme de contrôle d'admission basé sur des indicateurs de disponibilité des ressources par classe et globaux, ce qui les rend plus aptes à donner des décisions conséquentes avec la réalité du réseau.

Non sans peine, nous faisons une tentative de classement des scénarios en ordre décroissant de stabilité. Malgré les conjectures formulées, nous nous hasardons à le faire parce que le critère de stabilité revêt une importance considérable. Le troisième schéma et le deuxième peuvent sembler les plus stables parce que leur niveau de décision est centralisé; les réponses résultantes du PCF peuvent donc s'avérer plus cohérentes. Non loin derrière, on place la solution alternative du troisième schéma. Elle est moins stable que le deuxième si la fréquence des rapports périodiques envoyés au nœud centralisé BB est trop élevée. Le quatrième schéma est peut-être moins stable parce que ses processus de mesure et d'analyse sont co-localisés. De plus, les serveurs LPDP n'ont pas la richesse des politiques et la flexibilité décisionnelle du serveur PCF. Aussi, les perturbations dues à des changements réels dans le réseau risquent de blesser le système. Le premier scénario est peut-être plus versatile que ses concurrents, car ses processus d'acquisition des mesures et d'analyse sont élémentaires.

Cela dit, il n'est pas aisé d'évaluer ces scénarios en fonction du critère d'intérêt. Il serait intéressant de déterminer le classement par des simulations et grâce à un algorithme de vérification de stabilité [35]. Mieux encore, nous pourrions réaliser des tests d'implémentation pour obtenir des résultats plus concluants. Ceci est d'autant plus nécessaire que la position relative du premier schéma est floue. Pourtant, son potentiel de stabilité est proche de celui de 3GPP. Des tests ou des simulations permettraient donc de motiver ou non le choix d'un mécanisme plus élaboré.

Flexibilité

Pour comparer les scénarios suivant ce critère, nous rappelons trois éléments importants pour la flexibilité : le niveau d'indépendance entre les sous-

systèmes statiques et dynamiques (s'ils peuvent être activés et désactivés séparément ou non), la facilité de modifier la politique d'optimisation et la capacité d'accommoder différents scénarios de classes de trafic. Il faut rappeler que le PCF est censé être l'autorité décisionnelle, ce qui limite le niveau de flexibilité atteignable. En ce qui concerne la possibilité de modifier la politique d'optimisation, elle est bonne dans l'ensemble des scénarios, car elle est intimement liée au niveau d'automatisme que nous savons élevé pour l'ensemble des schémas. Un degré de flexibilité élevé peut donc être atteint si un haut niveau d'intelligence est incorporé dans les nœuds critiques du réseau, lesquels peuvent correspondre aux nœuds de politiques et ignorants de politiques. Mais ceci ne permet pas vraiment de classer les scénarios.

Quant au niveau d'indépendance d'action entre les modules statiques et dynamiques du système, il indique que le premier scénario est le plus flexible des cinq candidats. En effet, comme il est vraiment dynamique, des composantes statiques peuvent lui être intégrées plus aisément. Cependant, il faut souligner que tous les schémas supportent l'établissement, la modification et la fermeture des LSP dynamiques et statiques. Dans les quatre derniers, ces opérations peuvent être commandées par le PCF sur une base assez régulière. Donc, les LSP ont une durée de vie limitée, mais supérieure à celle d'une session unique. Ces scénarios sont donc caractérisés par un hybride de statisme et de dynamisme qui est étroitement lié à la gestion basée sur des politiques. En ce qui concerne la capacité des systèmes à accommoder différents scénarios de classes de trafic, les quatre derniers schémas sont sans doute plus aptes à le faire que le premier parce que leurs processus d'acquisition des mesures, d'analyse et d'optimisation considèrent des L-LSP. De surcroît, le critère de décision double apporte une valeur ajoutée parce qu'il différencie les classes de trafic temps réel et non temps réel.

À la lumière de ces observations, nous pouvons classer les schémas en ordre décroissant de flexibilité. Nous élisons d'abord le premier pour son dynamisme. Les autres solutions sont équivalentes, car leurs processus d'acquisition des mesures, d'analyse et d'optimisation se font aisément par l'entité décisionnelle PCF. Ces

solutions sont moins flexibles que la première, mais leur niveau d'automatisme leur confère une certaine capacité d'adaptation et donc une dose de flexibilité. Par exemple, dans ces solutions, les processus peuvent être désactivés en fonction des politiques définies. Entre autres, selon le schéma, le BB ou le serveur PCF ou le serveur LPDP peut ne pas solliciter les données si des conditions de politiques particulières sont respectées. Dans le deuxième schéma, le PCF peut ordonner au PEP de cesser d'envoyer des mesures (ACCTimer). De manière générale, pour les dernières solutions, le degré de flexibilité est étroitement lié au degré d'automatisme, et, donc, de la richesse des politiques définies par l'opérateur.

Visibilité

Les quatre derniers schémas sont plus visibles que le premier parce que les mesures sont globales et par classe, par opposition à celles par interface – et par classe - du premier scénario. En ordre décroissant de visibilité, nous élisons d'abord le troisième schéma, le deuxième et le quatrième ex æquo. Ensuite, nous choisissons la solution alternative du troisième schéma. Ce scénario dispose d'une connaissance du réseau morcelée dans le temps et les données reçues peuvent s'avérer moins représentatives. Le premier schéma succède aux autres parce qu'il se base sur des informations locales. Ce classement est déterminé par la facilité avec laquelle un diagnostic du réseau peut être établi à court terme et à long terme. Les requêtes bidirectionnelles peuvent révéler un problème de visibilité dans les scénarios basés sur un *Bandwidth Broker*.

Simplicité

Les scénarios utilisent le même mécanisme de contrôle d'admission basé sur des mesures. Le degré de complexité du module AC-KQ est supérieur à celui du AC-MVE. En ordre décroissant de simplicité, nous mettons en premier le schéma basé sur des E-LSP parce qu'il demande très peu d'ajouts par rapport au cadre générique de 3GPP. Ensuite, le deuxième schéma, le quatrième, le troisième et sa solution alternative sont aussi simples les uns que les autres. Nous pouvons placer le schéma COPS-Rpt en

dernier parce que le protocole COPS est encore immature.

Interopérabilité

À cet égard, les scénarios sont à peu près aussi inter-opérables les uns que les autres. Ils reposent sur des standards bien connus ou encore sur des éléments de 3GPP. Nous pouvons toutefois affirmer que les schémas faisant usage d'un BB présentent un inconvénient parce que le concept de BB ne fait pas l'objet d'un standard (problème de communication inter-BB).

Sécurité

L'aspect de sécurité n'est pas traité dans ce travail. À titre indicatif, COPS, SIP et SNMPv3 sont utilisés. Ils ont leurs propres mécanismes de sécurité. Mais, il existe des failles de sécurité répertoriées. Par exemple, aucune solution n'a été trouvée pour protéger le jeton d'autorisation d'un intermédiaire « untrusted ». De plus, actuellement, le contenu des messages SIP ne doit pas être encrypté. Ces deux lacunes affectent considérablement la sécurité globale du système et sont communes à l'ensemble des scénarios. Il ressort que les failles de sécurité peuvent conduire à la violation des autres recommandations, notamment à celles associées à la stabilité du système, à son évolutivité et à ses aspects plus fonctionnels tels que son contrôle de routage et sa survivabilité.

3.4.2 Comparaison des scénarios suivant les recommandations fonctionnelles

Quant aux recommandations fonctionnelles, elles décrivent les fonctions qui doivent être exécutées par le système d'ingénierie de trafic. Elles donnent des conseils relativement au contrôle de routage, à l'affectation du trafic à un chemin, au sous-système de mesures et, enfin, à la survivabilité du réseau. Un compromis acceptable doit être trouvé entre les contraintes posées par ces recommandations, contraintes dont les priorités doivent être prises en compte lors du design du système d'ingénierie de

trafic. Dans les lignes qui suivent, nous comparons les scénarios à l'aide des recommandations fonctionnelles.

Contrôle de routage et affectation de trafic à un chemin

Nous traitons à la fois du contrôle de routage et du processus d'affectation du trafic à un chemin parce qu'ils apparaissent quasi-indissociables. D'emblée, l'algorithme CBR est utilisé par les cinq schémas, ce qui leur permet de composer avec les contraintes liées à l'état du réseau et aux exigences de QdS des applications. Dans les quatre derniers scénarios, en réalité, les routes sont calculées à l'avance et les LSP sont préétablis sur cette base. Cependant, les tables FTN sont mises à jour pour une requête admise ou pour respecter une politique événementielle ou temporelle quelconque. De plus, les tables FTN des nœuds GSN contiennent plusieurs LSP par FEC et la sélection d'un LSP - et donc d'une route - dépend de la décision de l'algorithme de contrôle d'admission basé sur des mesures. Pour ainsi dire, les deux processus reposent sur la richesse des politiques explicitées par l'opérateur et sur la qualité des sous-systèmes d'acquisition des mesures et d'analyse. Il est donc difficile de déclarer un classement des scénarios en raison de la quantité de données inconnues et difficilement estimables. La stabilité est un facteur qui détermine grandement la performance des deux sous-systèmes. Sans doute, un écart de performance existe entre le premier schéma et les autres. De plus, une panne peut compliquer les choses si le dimensionnement et la gestion des LSP sont inadéquats. Le problème est exacerbé dans le cas d'une requête bidirectionnelle.

Mesures

En ce qui concerne les processus d'acquisition des mesures et d'analyse, ils sont affectés par plusieurs facteurs. D'emblée, les schémas emploient le même mécanisme de contrôle d'admission basé sur des mesures. Leurs paramètres doivent être bien choisis. Les quatre derniers schémas sont plus visibles que le premier. Donc, en ordre décroissant, nous pouvons élire ex æquo le troisième schéma et le deuxième si la

fréquence des rapports périodiques est raisonnable. Ces deux schémas fournissent la totalité des mesures prélevées au nœud principal de gestion des ressources (malgré leur manque d'évolutivité). Après, le quatrième schéma peut fournir des indicateurs de disponibilité des ressources plus justes, mais il peut s'avérer moins évolutif. Ensuite, la première solution alternative peut être choisie. La base MIB de son BB (PCF) ne contient pas toutes les mesures acquises par le processus concerné et elle peut avoir des données peu représentatives du réseau. Le premier scénario dispose des plus pauvres sous-systèmes parce que ses mesures ne sont pas globales.

Survivabilité

En matière de survivabilité, les cinq schémas semblent comparables. Les méthodes classiques prévues par 3GPP et celles liées aux technologies déployées sont utilisées. Entre autres, les nœuds GSN, BB et PCF disposent de serveurs de backup et sont robustes (multi-processus, etc.). Des LSP alternatifs sont prévus. Les méthodes de protection et de restauration de MPLS sont aussi employées. De plus, le serveur local de politiques peut cacher des décisions et remplacer le serveur PCF en cas de déconnexion transitoire (tolérance aux pannes). De manière générale, la gestion basée sur des politiques peut améliorer la survivabilité, car elle peut préciser des conditions de politiques proactives et réactives liées à des événements de pannes et spécifier des actions de politiques conséquentes (proactives et réactives). Ceci est encore plus vrai pour les quatre derniers scénarios qui reposent fondamentalement sur les mises à jour à moyen terme des tables FTN, lesquelles sont commandées par les décisions synchrones et asynchrones du PCF (inscription d'une requête, politique temporelle ou événementielle). Néanmoins, les failles de sécurité dans UMTS peuvent détériorer la survivabilité du système, notamment les attaques de déni de service et de violation de confidentialité. Enfin, si la décentralisation a ses vertus, elle s'accompagne généralement de contraintes matérielles et logicielles pas toujours faciles à accepter.

Au terme de cet exercice de comparaison, nous constatons que certaines recommandations ne permettent pas toujours de classer les schémas de fonctionnement.

De plus, certains aspects du réseau sont hors de la portée de ce document. Il faudrait recourir à des tests ou à des simulations. Cela dit, le système d'ingénierie de trafic souhaité doit trouver un compromis acceptable entre les contraintes posées par les recommandations susmentionnées, car celles-ci n'ont pas la même importance et peuvent être antagoniques. Dans un contexte donné, certaines peuvent devenir critiques et d'autres optionnelles. Les priorités relatives de celles-ci doivent donc être rigoureusement respectées lors de la phase de design.

3.5 Choix de la solution retenue

Après examen des scénarios, il ressort que le premier schéma est incapable de fournir des bornes acceptables sur les garanties de QdS. Nous choisissons donc de l'écarter malgré ses résultats de classement. Pour les fins visées par le mécanisme de contrôle d'admission basé sur des mesures, le schéma préconisé est le troisième. Il utilise un *Bandwidth Broker* et repose sur des mises à jour périodiques SNMP pour alimenter son processus d'analyse. Ce scénario est donc retenu parce qu'il semble stable et parce qu'il dispose d'un processus d'acquisition des mesures consistant, apte à fournir des indicateurs d'utilisation des ressources à court terme et à moyen terme. De surcroît, il est plus conforme à l'IETF. Le processus d'analyse employé est fondé sur le mécanisme AC-MVEv2 ou AC-KQv2. La solution proposée enrichit la gestion de 3GPP, car elle repose sur des politiques riches. De plus, elle permet de supporter une variété de niveaux de QdS en vue de livrer la qualité de service souhaitée par le client.

CHAPITRE 4
IMPLÉMENTATION ET RÉSULTATS

L'exercice de comparaison réalisé au chapitre précédent a permis de dégager une solution susceptible de composer avec les contraintes antagoniques d'utilisation des ressources et de respect de la qualité de service souhaitée par les applications. À titre de rappel, la solution retenue inclut un *Bandwidth Broker* qui implémente les processus d'acquisition des mesures et d'analyse, lesquels sont basés sur les données des L-LSP récupérées par le *Bandwidth Broker* sur une base régulière. Pour des raisons diverses, particulièrement liées aux inconnues dans 3GPP et aux lacunes que présente le logiciel retenu, une évaluation de performance partielle est réalisée pour le volet unique de « disponibilité des ressources ». La solution proposée n'est donc validée qu'en partie, car le réseau de base employé est filaire et uniquement basé sur les technologies MPLS et DiffServ. De plus, le module MBAC AC-MVEv2 est le seul mécanisme implémenté. Notre solution est comparée à un schéma de fonctionnement dont la teneur en mécanismes de QdS se rapproche de celle de 3GPP (OPNET). Ce chapitre fournit d'abord les détails d'implémentation. Après le plan d'expériences, il présente les résultats des scénarios, et une comparaison de ceux-ci en fonction des métriques et des facteurs des expériences de simulation. Il se termine sur une section d'inférences pour UMTS.

4.1 Détails d'implémentation

Avant toute chose, il est important de préciser certains détails d'implémentation. Cette section relate des informations pertinentes sur l'environnement matériel et logiciel de support, l'environnement de simulation et le code.

4.1.1 Environnement matériel et logiciel

Pour ce travail, la version 10.5 du logiciel OPNET a été employée. Cet environnement de développement permet de concevoir et d'étudier le comportement des réseaux. OPNET est fondé sur une approche orientée objet. Ce logiciel fournit le code source de sorte qu'il est possible de rédiger des extensions. Il est particulièrement prisé dans la communauté scientifique, pour les fins de recherche et autres. Il définit trois domaines, soient les domaines réseau, nœud et processus. Le premier se définit autour des différents éléments qui le constituent, notamment de ses liens, nœuds et objets de configuration globaux. Le second domaine illustre l'architecture interne d'un nœud d'un point de vue fonctionnel. À ce niveau sont donc détaillés les modules de contrôle et de transmission que l'entité invoque dans l'exercice de ses fonctions. Le troisième domaine constitue la machine à états finis d'un processus. Noter que le processus en question peut être appelé par un module d'un nœud de manière directe ou indirecte. Enfin, il faut remarquer que la simulation se fait par événements discrets, c'est-à-dire que le temps avance uniquement lorsqu'un processus est invoqué. Le Tableau 4.1 montré ci-dessous résume les informations décrivant l'environnement matériel et logiciel de support.

Tableau 4.1 Information système

Information système	
Version	10.5.A PL3 (Build 2570)
Type d'hôte du système	WIN32
Information sur l'hôte	Windows NT 5.0 Build 2195
Architecture du processeur	0
Nombre de processeurs	1
Type de processeur	586
Niveau du processeur	15
Révision du processeur	521
Mémoire physique totale	1048076 Ko
Mémoire physique libre	697252 Ko

4.1.2 Adaptation de l'environnement de simulation

En vue de modéliser la charge et le système d'ingénierie de trafic suggéré, il s'est avéré nécessaire de procéder à une adaptation de l'environnement de simulation. Ci-après, nous motivons les artifices d'implémentation réalisés et la représentation adoptée pour notre solution. Les détails d'adaptation essentiels sont ensuite précisés.

Motivation des artifices d'implémentation et de la représentation de la solution

Le logiciel OPNET ainsi que les documents de 3GPP et de l'IETF ne fournissent pas des éléments de réponse à tous nos questionnements. Dans les spécifications d'UMTS et de l'IETF, certaines informations sont expliquées en surface et d'autres ne sont pas fournies. Certaines données peuvent faire l'objet de documents à venir et d'autres peuvent constituer pour les rédacteurs des spécifications des détails superflus. Force est de constater que la version d'UMTS considérée dans ce travail n'est pas destinée à être commercialisée. Parmi les questions peu claires de cette version, citons celle de la mise en correspondance des paramètres SDP avec les politiques et celle du contenu des politiques des serveurs global et local (PDP et LPDP). Pour l'IETF, relevons le concept de *Bandwidth Broker* qui n'est toujours pas réglé en définitive.

En plus des problèmes précités, s'ajoutent ceux liés aux lacunes ou artifices de développement propres à OPNET. Le code dissimule parfois des incohérences, comporte des modules incomplets et inclut quelques fois des procédures qui s'enlignent difficilement avec les objectifs de notre travail. Par exemple, le module SNMP comprend un processus vide. Ensuite, le processus umts_gtp ne spécifie pas correctement les valeurs ToS pour les tunnels GTP. De plus, il est actuellement impossible d'effectuer une réservation consistante de largeur de bande pour des LSP statiques – voire dynamiques - et, naturellement, les LSP de type L-LSP ne sont pas supportés. Quant aux entités et procédures propres à la version 5 de normalisation d'UMTS, elles ne sont pas implémentées (COPS, SIP et autres) et, ce, pour des raisons que nous imaginons diverses et surtout liées au caractère transitoire de cette version de recherche.

En conséquence, une preuve de concept partielle est réalisée pour le volet unique de « disponibilité des ressources » du schéma de fonctionnement proposé. Une abstraction du *Bandwidth Broker* est effectuée afin de simplifier les processus d'acquisition des mesures et d'analyse. L'implémentation SNMP se résume à une collecte des mesures des LSP dans des structures de données propres aux nœuds en périphérie du domaine. De plus, en lieu et place d'un réseau UMTS augmenté des technologies MPLS et Diffserv, un réseau MPLS – DiffServ est employé. Si cette représentation de la solution présente des inconvénients, elle n'en permet pas moins de réaliser une preuve de concept intéressante pour UMTS (après extrapolation). En effet, le domaine d'intérêt du réseau UMTS est le domaine à commutation de paquets du réseau de cœur.

Détails relatifs à l'adaptation de l'environnement de simulation

L'environnement de simulation a été adapté en vue de pallier les lacunes susnommées et de simplifier l'analyse. Entre autres choses, chacun des LSP statiques se voit attribuer la totalité de la largeur de bande, à l'exception des LSP symétriques vidéo sur demande qui partagent plus ou moins équitablement la capacité des liens. Les LSP sont donc généralement placés sur des interfaces différentes des nœuds LER. Si cette astuce a ses conséquences sur l'évaluation de performance, elle permet cependant de remédier au problème de réservation de largeur de bande pour un LSP. Les capacités pour les liens sont spécifiées avec des nombres et ne sont donc pas déterminées avec des liens standards (OC-192, DS3, etc.). De plus, chaque LSP convoie un agrégat de flots d'une classe unique de qualité de service (L-LSP). Le trafic est de type vidéo sur demande ou de type http, respectivement de qualité de service AF11 ou AF31. Plusieurs applications pour la vidéo sur demande sont définies à l'aide des traces d'une archive communément utilisée par les chercheurs [36]. Les traces choisies possèdent un paramètre de Hurst supérieur à 1.5 et un débit variable, ce qui assure en leur sein une composante d'auto-similarité. Elles consistent en les films Silence of the Lambs, Star Wars, Mr Bean, The Firm et Die Hard III. Différents profils sont développés, les uns

incluent une application unique pour le flot d'une source requête, les autres, un agrégat d'applications pour le flot d'une source de trafic en cours. Mais, les profils sont expliqués plus tard.

En outre, les applications de trafic http sont obtenues à partir d'une trace correspondant à un agrégat de flots. La distribution pour les arrivées et celle pour la taille des objets sont celles de la trace EPA-HTTP de l'archive Internet [37]. Cette trace contient au total 47748 requêtes pour un serveur occupé. Ici aussi, des profils sont définis pour des sources symbolisant des requêtes et d'autres sont spécifiés pour modéliser des sources de trafic en cours. Dans le premier cas, la séquence des requêtes d'un seul hôte est considérée tandis que, dans le second, c'est une portion de la trace entière qui est prise en compte (tous hôtes confondus). Les fichiers des traces ont été adaptés pour OPNET. Ces traces http et vidéo sur demande sont utilisées parce que nous avons la certitude qu'elles possèdent les composantes de dépendance à long terme et d'auto-similarité. Ces propriétés excentriques dans le trafic sont nécessaires pour mettre sous tension l'algorithme de contrôle d'admission proposé.

En ce qui concerne le modèle réseau d'OPNET, il est relativement simple. Du côté du nœud LER d'entrée, les sources http englobent une source modélisant le trafic en cours et deux sources symbolisant des requêtes. Du côté du nœud LER de sortie, elles regroupent plutôt un serveur pour les requêtes et un serveur pour le trafic en cours. En ce qui concerne le trafic vidéo sur demande, il est généré des deux côtés par une source requête et une source de trafic en cours. Le modèle OPNET du réseau est montré à la Figure 4.1. Les fluctuations du trafic sont étonnantes et particulièrement grandes en amplitude pour le trafic de type http. Les valeurs des liens de base du réseau sont donc obtenues à l'issue de plusieurs simulations. Le processus itératif a permis d'ajuster les valeurs des liens du réseau pour obtenir une utilisation proche de 0.7 % (« critère d'arrêt »). Le scénario générique obtenu est sans biais particulier et il véhicule la quasi-totalité du trafic. Ceci a permis d'éviter les erreurs de simulation qui voulaient insinuer le séjour de certains émetteurs TCP dans des phases de contrôle de congestion avancées. Le Tableau 4.2 fournit les valeurs des liens employées par le réseau de base.

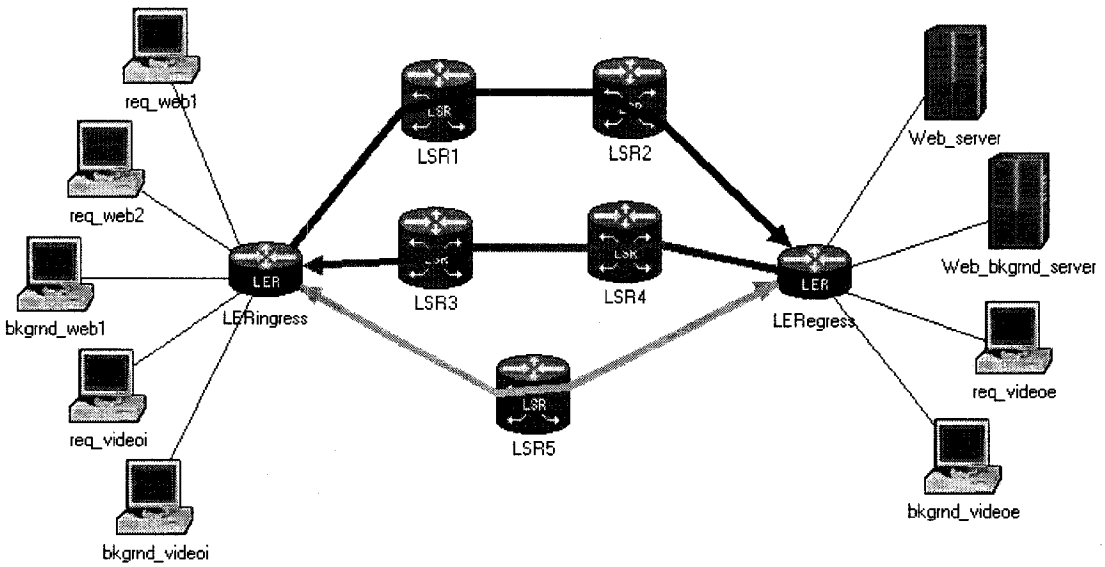

Figure 4.1 Topologie du réseau de base considéré

Tableau 4.2 Liens de base des LSP

LSP	*Valeurs des liens sur le LSP (Mbps)*
LSPhttp1 (liaison montante)	12
LSPhttp2 (liaison descendante)	28
LSPvideo1, LSPvideo2	41,000

Les paramètres des profils de QdS sont indiqués au Tableau 4.3. Ils ont également été obtenus après plusieurs itérations. Ils sont permissifs afin d'éviter une mise en forme substantielle de l'auto-similarité du trafic. En effet, cette composante et celle de dépendance à long terme sont nécessaires pour apprécier notre algorithme de contrôle d'admission.

En ce qui concerne les poids WFQ pour les classes AF11 et AF31, ils égalent respectivement 70 et 30. Quant aux valeurs pour les tailles des tampons et des files

d'attente, elles conservent les valeurs par défaut spécifiées par le logiciel (500 paquets et 1 Mo).

Tableau 4.3 Profils de QdS des sources du réseau

Trafic	*Profil de QdS [débit max (Kbps), débit moy (Kbps), taille rafale (Kb), action non conformité]*	
http	Requête	[100, 50, 50, rejeter]
	Serveur requête	[500, 250, 250, rejeter]
	Trafic en cours	[300, 150, 150, rejeter]
	Serveur trafic en cours	[1 500, 750, 750, rejeter]
Vidéo sur demande	Requête	[50 000, 25 000, 25 000, rejeter]
	Trafic en cours	[300 000, 150 000, 150 000, rejeter]

Adaptation du code

Dans OPNET, le module IP lance le processus ip_dispatch au début de la simulation. Ce processus constitue un répartiteur qui, au besoin, crée et invoque des processus fils pour leur déléguer des tâches généralement complexes. Entre autres choses, il crée et invoque un processus mpls_mgr dans tous les nœuds MPLS pour se dispenser du traitement des paquets avec un en-tête MPLS. Le traitement se résume à une vérification de conformité du paquet reçu vis-à-vis d'un profil de QdS. De plus, si des LSP statiques sont déployés, aucun message de signalisation n'est convoyé à l'effet de distinguer les nouveaux flots des anciens. De surcroît, un mécanisme de contrôle d'admission n'est pas implémenté. Ces constations expliquent l'adaptation du code pour effectuer l'analyse et l'acquisition des mesures.

Pour des raisons pratiques, les procédures de l'analyse MBAC sont disséminées dans le code du processus mpls_mgr. L'acquisition des mesures est accomplie par le

nouveau processus mg_msrt_process qui est hébergé par le module SNMP d'un nœud LER. Il est créé et invoqué par mpls_mgr. Les deux processus communiquent à l'aide du mécanisme de mémoire parent-enfant. La structure de données accédée renferme essentiellement les mesures des LSP. Elle constitue une variable d'état qui est initialisée par le processus mpls_mgr. L'adresse de cette structure est passée au processus fils afin de lui permettre de s'acquitter de ses fonctions. Il la met à jour sur une base régulière suivant une période d'échantillonnage de trois millisecondes. La structure est par la suite consultée par le processus père avant de répondre à une requête de contrôle d'admission. Ce processus implémente donc l'estimateur et le critère de décision du mécanisme de contrôle considéré.

En fait, le contenu du bloc mémoire accédé est de type msrt_LSP. Le format de cette structure conserve, pour chaque classe de qualité de service, un pointeur vers une liste de variables qui pointent à leur tour vers des structures de type msrt_LSP_per_class (List* msrt_class_AF11 et msrt_class_AF31). Chacune renferme le nom du LSP, sa classe de qualité de service, le tableau de mesures des LSP de l'algorithme AC-MVEv2, l'unité de mesure la plus récente associée au LSP, l'index de la prochaine case à mettre à jour dans le tableau de mesures et, enfin, un pointeur vers une liste d'éléments de type Fec_unit_LSP. Ce dernier élément précise une série d'informations rattachées à un FEC, soient le nom du FEC, son interface d'entrée, sa classe de QdS, le débit maximum autorisé dans son profil, l'instant de la prochaine requête, la position de la prochaine case à lire dans le tableau des arrivées, la position de la prochaine case à lire dans le tableau des départs pour le FEC, l'occurrence du départ d'un flot sur l'interface concernée par le FEC et, finalement, une variable indicatrice du rejet d'une requête sur cette même interface dans le passé. Les deux dernières variables sont examinées par le critère de décision en mode P-BP (pour les requêtes de type AF11). La dernière est initialisée à zéro et mise à un lorsqu'un refus est émis par le mécanisme d'admission et remise à zéro lorsqu'un flot de la classe quitte le système. Les paquets qui suivent une « requête » AF11 refusée sont donc éliminés jusqu'à ce qu'un départ soit constaté pour

un flot de la classe AF11. Et, de manière générale, les paquets des deux classes sont écartés s'ils sont associés à une requête non admise.

Comme il a été dit précédemment, le réseau employé supporte les technologies MPLS, DiffServ et fait usage de LSP statiques. Ainsi, il n'utilise pas de protocole de signalisation pour établir des connexions, c'est-à-dire que les protocoles RSVP et LDP ne sont pas utilisés. En conséquence, la dynamique des entrées et des départs des flots ne peut pas être suivie. Aussi, l'algorithme a besoin d'une connaissance de cette dynamique. De plus, le système ne véhicule pas de requêtes d'activation ou de modification de contexte PDP. À titre de rappel, ce sont ces requêtes qui conduisent à l'exécution du mécanisme de contrôle d'amission. Mais, nous avons déjà vu que le réseau UMTS et le système MPLS avec LSP dynamiques sont modélisés de manière artificielle par OPNET. Les adaptations effectuées visent à réaliser la preuve de concept et à pallier les problèmes précités.

Ainsi, deux artifices d'implémentation sont réalisés. Le premier a trait à la dynamique des arrivées et départs des flots du système et le second, aux flots refusés. Dans le premier, l'algorithme calcule les inter-arrivées des requêtes sur les interfaces des FEC à l'aide d'une distribution exponentielle. Les paramètres sont choisis parce que ceux des traces ne sont pas connus; ils égalent 50 et 100 respectivement pour les sources http et vidéo sur demande. Quant aux occurrences des départs des flots AF11, elles sont également choisies de manière aléatoire. Les départs et les arrivées des flots par interface (par FEC) sont conservés dans les champs de la structure Fec_unit_LSP et sont mis à jour au fur et à mesure à l'aide de ces valeurs. Mais, dans la réalité, ces informations sont véhiculées dans les requêtes d'activation, de modification et de fermeture de contexte PDP. Le Tableau 4.4 dresse une liste des structures principales. Celles-ci permettent de réaliser les artifices ainsi que les processus d'analyse et d'acquisition des mesures.

Le Tableau 4.5 présente un sous-ensemble des structures d'OPNET employées. Une variable non montrée est, par exemple, la structure MplsT_NHLFE d'OPNET. Elle contient les informations relatives à une entrée NHLFE, notamment un pointeur vers la

liste des entrées FEC associées au NHLFE, le nom du LSP, sa largeur de bande et une série de statistiques pour le délai, les niveaux de charge en bits/s et en paquets/s et d'autres informations utiles. Ainsi, les structures susmentionnées sont largement manipulées par nos processus de collecte des mesures et d'analyse.

Tableau 4.4 Structures de données définies

Structures de données définies

mg_msrt_process.h

```
typedef struct
 {
 char       lsp_name[256];
 (double    msrtsKQ[TailleFenetreKQ];)
 double     msrtsMVE[TailleFenetreMVE];
 double     unit_msrt;
 (int       curr_indexKQ;)
 int        curr_indexMVE;
 List*      fec_list;
 int        classe_QdS;
 }msrt_LSP_per_class;

typedef struct
 {
 List* msrt_class_AF11;
 List* msrt_class_AF31;
 } msrt_LSP;
```

```
typedef struct
 {
 char*      fec_name;
 int        fec_in_face;
 int        tos;
 double     peak_rate;
 int        refusal;
 double     next_req_schedule_time[51];
 int        depart[51];
 int        index_depart;
 int        tab_index_next_req;
 }Fec_unit_LSP;
```

Avant toute chose, rappelons que les requêtes bidirectionnelles http sont initiées seulement du côté du nœud d'entrée LER et que les requêtes unidirectionnelles vidéo sur demande sont générées des deux côtés du domaine. Il s'ensuit que les premières requêtes exigent une évaluation de la disponibilité des ressources sur les liaisons montante et descendante, tandis que les requêtes vidéo sur demande conduisent à une évaluation sur une liaison simple.

Tableau 4.5 Structures de données d'OPNET

Structures de données d'OPNET

mpls_support.h

```
typedef enum
    {
    MplsC_TC_Action_Discard,
    MplsC_TC_Action_Shape,
    MplsC_TC_Action_Transmit,
    MplsC_TC_Action_Transmit_Remar
    ked
    } MplsT_TC_Action;

typedef struct
    {
    double max_bit_rate;
    double avg_bit_rate;
    double max_burst_size;
    } MplsT_Traffic_Profile;

typedef struct
    {
    MplsT_TC_Action action;
    int remark_value;
} MplsT_Policy_Action;
```

```
typedef struct
    {
    char* trunk_name;
    int traffic_class;
    MplsT_Traffic_Profile*
    traffic_profile_ptr;
    MplsT_Policy_Action* policy_action_ptr;
    } MplsT_Traffic_Trunk;

typedef struct
    {
    int tos;
    int protocol;
    IpT_Address_Range* src_addr_range_ptr;
    IpT_Address_Range*dest_addr_range_ptr;
    int src_port;
    int dest_port;
    int in_iface;
    char*fec_name;
    int parsed_iface;
} MplsT_Fec_Info;
```

mpls_mgr.h

```
typedef struct
   {
   Packet* pkt_in;
   MplsT_NHLFE* nhlfe_ptr;
   MplsT_Shim_Header* shim_header;
   int traffic_class;
   int in_iface;
   int instrm;
} MplsT_Forward_State;
```

```
typedef struct
    {
    MplsT_NHLFE* nhlfe_ptr;
    int* nhlfe_is_set;
    Objid lsp_objid;
    List* mapped_fecs_lptr;
    int failed_objects_count;
  } MplsT_Lsp_Desc;
```

Cela dit, dans notre implémentation, un paquet est par défaut soumis à un module de vérification de conformité, mais l'opération est effective en définitive uniquement si le paquet est membre de la classe AF11 et lié à un flot accepté ou encore s'il est de la classe AF31 et associé à une requête autorisée (la variable globale DL_gateAF31 est la porte de discrimination des flots http autorisés). Mais, l'algorithme vérifie toujours s'il doit d'emblée écarter le flot - et le rejeter - ou s'il doit exécuter le test de contrôle d'admission. Un paquet AF11 n'est pas éligible au test de contrôle d'admission et est automatiquement rejeté s'il est associé à un flot refusé et qu'aucun flot de sa classe n'a quitté le système. Un paquet AF31 subit le même sort si la porte DL_gateAF31 est fermée. Noter que la variable globale est mise à jour pour refléter l'admission ou le refus d'une requête. AC-MVEv2 peut décider d'accepter une requête ou de la refuser. Les paquets générés par les sources de trafic en cours ne sont en aucun cas soumis au mécanisme de contrôle d'admission; ils sont sujets à des opérations de vérification de conformité. Pour ainsi dire, le processus d'analyse peut refuser un flot, le transmettre ou encore vérifier sa conformité avec son profil de QdS correspondant. La Figure 4.2 illustre le traitement des paquets d'un point de vue fonctionnel, c'est-à-dire sans les particularités et les artifices d'implémentation réalisés.

Cela dit, les procédures pour l'analyse sont disséminées dans le code du processus mpls_mgr. Elles se trouvent dans l'exécutive de sortie de l'état init_wait et dans les fonctions *mpls_mgr_packet_process()*, *mpls_mgr_packet_forward()*, *mpls_mgr_packet_in_stats_write()* et *mpls_mgr_lsps_parse()*.

4.2 Plan d'expériences

Dans le but d'évaluer la viabilité du système d'ingénierie de trafic proposé, un plan d'expériences doit être suivi scrupuleusement. Cette section est donc consacrée à sa description. Elle précise les hypothèses simplificatrices, les métriques considérées ainsi que les facteurs et les niveaux de ceux-ci. Elle explicite ensuite les expériences de simulation.

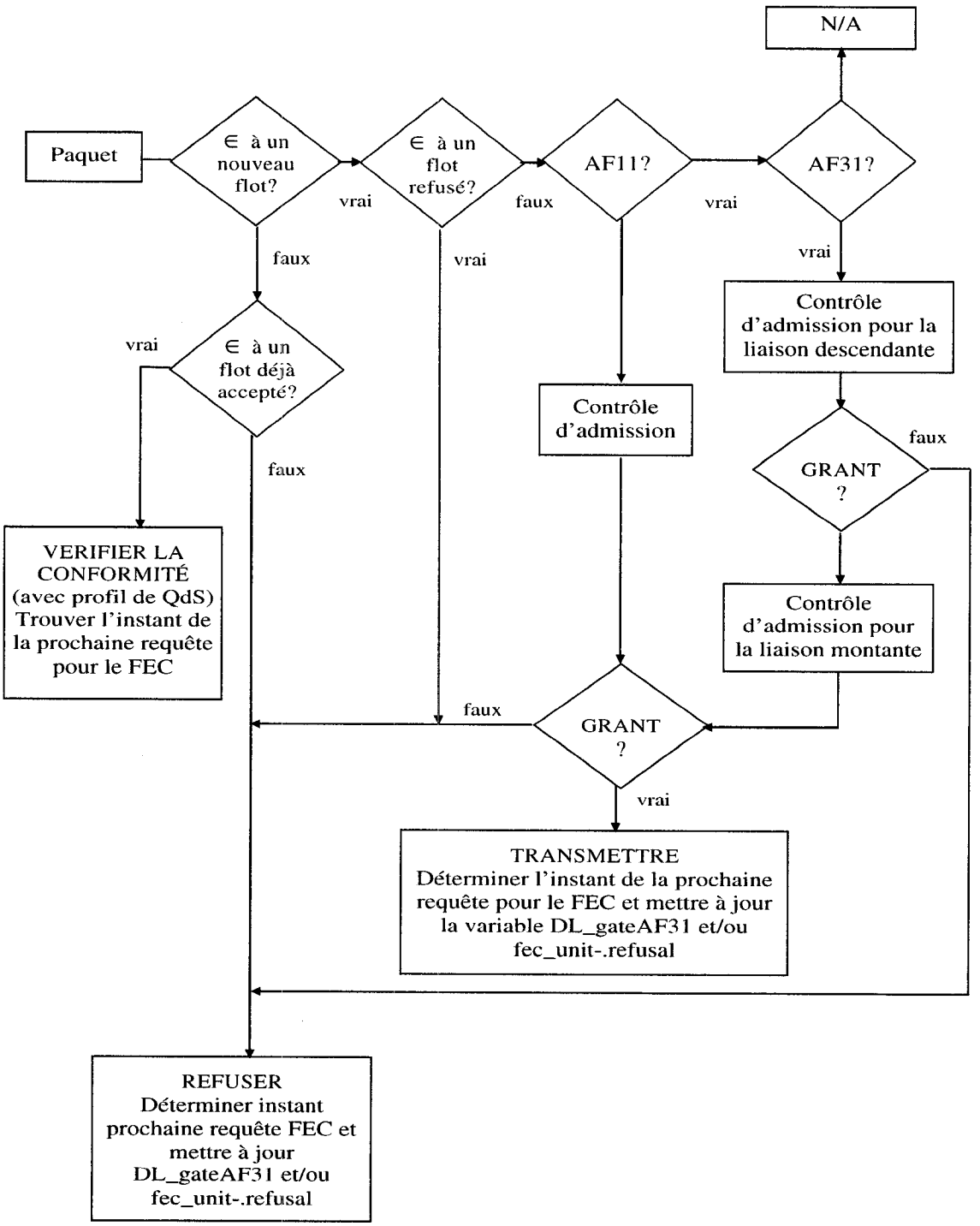

Figure 4.2 Diagramme de fonctionnement du code de traitement des paquets

4.2.1 Hypothèses

L'évaluation de performance repose sur des hypothèses simplificatrices ici indiquées. Celles-ci sont liées à une variété d'éléments, tels que les usagers et les paramètres de configuration. Elles sont brièvement expliquées.

Dans notre modèle, les conjectures suivantes sont formulées :

- Le domaine d'interconnexion des usagers supporte les technologies MPLS et DiffServ. Il comprend les nœuds d'entrée et de sortie LER et cinq nœuds LSR.

- La taille de la file d'attente est de 500 paquets et la taille du tampon vaut 1 Mo. Ces valeurs ne sont pas réalistes, mais elles constituent les valeurs par défaut du logiciel.

- Les liens qui connectent les sources aux nœuds périphériques LER sont de type SONET-OC192. Le surdimensionnement de ces liens permet d'éviter toute congestion dans l'accès. Les autres liens possèdent des capacités différentes.

- Les LSP sont statiques et représentent des L-LSP. Toutefois, ce type de LSP n'est pas supporté dans OPNET et la réservation de largeur de bande pour un LSP statique est inconsistante. Aussi, dans le but de remédier aux lacunes du logiciel et de respecter le caractère asymétrique des liaisons bidirectionnelles, nous plaçons les LSP sur des chemins disjoints et nous leur appliquons les règles de QdS. Les réservations sont faites indirectement, c'est-à-dire en dimensionnant les liens des LSP. Le LSP http sur la liaison montante ne partage pas les liens du LSP sur la liaison descendante, contrairement aux LSP vidéo sur demande qui sont plus ou moins symétriques. Ceci permet aussi de pallier le degré limité de connexité des nœuds LER.

- Des sources vidéo sur demande sont employées pour fournir un trafic en temps réel avec des exigences dures en QdS et des sources http sont utilisées pour véhiculer un trafic non temps réel avec un degré de tolérance élevé pour les dégradations non persistantes de la qualité de service. Les premières, sensibles au délai et à la gigue, appartiennent à la classe conversationnelle d'UMTS. Les dernières sont incluses dans la classe en arrière-plan et sont plutôt sensibles au taux de perte. Les requêtes http sont bidirectionnelles, par opposition aux requêtes vidéo sur demande qui sont unidirectionnelles.

- Les clients http regroupent, pour la liaison montante, deux sources qui modélisent les requêtes http (req_web1 et req_web2) et une source qui correspond au trafic en cours (bkgrnd_web1). Les sources « requêtes » utilisent respectivement les séquences des hôtes keyhole.es.dupont.com et dcimsd23.dcimsd.epa.gov (de la trace epa-http). Pour la liaison descendante, ces clients incluent une source qui représente le trafic de réponse aux requêtes des usagers et une autre qui fournit le trafic de réponse au trafic en cours http (Web_server et Web_server_bkgrnd). Une portion de la trace est alors utilisée.

- En ce qui concerne les clients vidéo sur demande, ils comprennent les sources req_videoi, req_videoe, bkgrnd_videoi et bkgrnd_videoe. L'interprétation de ces sources est analogue à celle pour les clients http, c'est-à-dire que les deux premières sources modélisent les requêtes et les dernières, un type de trafic en cours. Les applications Verbose Silence of Lambs VBR et Terse Silence VBR sont utilisées par les req_videoi et req_videoe respectivement. Les sources de trafic en cours consistent en un agrégat des sept traces.

- Pour des raisons déjà citées, les inter-arrivées des FEC et les départs des flots sont déterminés à l'aide de distributions aléatoires. Pour les flots http, la source de trafic en cours modélise un ensemble d'usagers qui alternent entre des périodes actives et inactives. Les fichiers pour les sources modélisant des requêtes correspondent à une portion du trafic d'un hôte tiré de la trace EPA-HTTP qui se trouve tantôt en phase active tantôt en phase inactive. En ce qui concerne la dynamique des sources vidéo sur demande, elle est tout autre, car les flots ne quittent pas le système. Nous avons préféré faire cela afin de ne pas avoir à trouver des paramètres pour décrire la durée des applications – de peur que ceux-ci s'avèrent inadéquats. Nous pouvons imaginer que les arrivées et départs des flots sont denses et associés à des clips vidéo sur demande de courte durée.

- Par ailleurs, le temps de simulation est fixé à 20 minutes afin de permettre le traitement d'un nombre raisonnable de requêtes.

Le ratio des clients http versus les clients vidéo sur demande n'est pas conforme aux spécifications précisées dans UMTS. En effet, le ratio considéré sous-estime le nombre de clients http. Néanmoins, et malgré les autres hypothèses, notre but est de placer le réseau dans un état de congestion et de regarder les dégradations de QdS qui peuvent s'ensuivre pour les flots des classes temps réel et non temps réel. Les objectifs de l'évaluation de performance ainsi que les métriques et facteurs des expériences de simulation sont choisis en conséquence.

4.2.2 Métriques, choix des facteurs et de leurs niveaux

Intrinsèques à une évaluation de performance sont les métriques et les facteurs. Cette section traite de ces éléments fondamentaux des expériences de simulation. Les niveaux des facteurs sont aussi précisés.

Pour les fins visées par notre étude, les métriques choisies incluent le délai, la gigue, le taux de perte et l'utilisation. Les quatre sont déterminées par classe. Quant aux facteurs, ils regroupent le type de mécanisme de contrôle d'admission et le facteur d'augmentation de trafic d'un LSP. Le taux de perte est égal à la différence entre les débits moyens d'entrée et de sortie du LSP sur le débit moyen d'entrée du LSP. Les niveaux des facteurs sont donnés au Tableau 4.6.

Tableau 4.6 Niveaux des facteurs

Facteurs	*Niveaux des facteurs*
Mécanisme de contrôle d'admission	[AC-MVE, aucun (OPNET)]
Facteur d'augmentation de trafic d'un LSP (multiple)	[1, 100, 500, 1000, 1100]

Les niveaux de congestion sont modérés afin de pallier les artifices d'implémentation et l'adaptation de l'environnement de simulation, particulièrement ceux liés à l'artifice qui consiste à rejeter les flots refusés au niveau du nœud frontière LER et de l'artifice qui donne une dynamique des arrivées et départs des flots. Les

métriques sont donc examinées pour des valeurs différentes d'augmentation du trafic dans les LSP.

4.2.3 Description des expériences de simulation

Les expériences de simulation se définissent autour des éléments susnommés, c'est-à-dire des métriques et des facteurs. Ci-après, nous décrivons les scénarios de notre évaluation de performance.

Pour les fins de comparaison, le schéma d'OPNET est utilisé. Il peut être rapproché de celui de 3GPP en raison de sa teneur limitée en mécanismes de QdS. Il ne possède pas de module de contrôle d'admission complet pour le volet « disponibilité des ressources ». Dans cette étude, nous évaluons le compromis en termes d'utilisation des ressources et d'offre de QdS qui est réalisé par les scénarios. Le Tableau 4.7 détaille les expériences de simulation.

Tableau 4.7 Expériences de simulation

		Scénarios	
		(1 - 5)	*(6 - 10)*
Facteurs	*Mécanisme de contrôle*	AC-MVE	Aucun (OPNET)
	Facteur d'augmentation de trafic	[1, 100, 500, 1000, 1100]	[1, 100, 500, 1000, 1100]
Métriques	*Délai*	X	X
	Gigue	X	X
	Taux de perte	X	X
	Utilisation	X	X

Le facteur d'augmentation de trafic est ajusté en modifiant les valeurs des liens. Les liens initiaux sont divisés par ce facteur pour simuler une augmentation du trafic. Avec les résultats des expériences de simulation, nous tenterons d'inférer la qualité de nos propositions par rapport à la solution de 3GPP. À titre de rappel, celle-ci est caractérisée par un module de contrôle d'admission que nous jugeons incomplet.

4.3 Résultats de simulation

Les expériences de simulation donnent des résultats différents pour notre proposition et celle d'OPNET. Cette section présente les valeurs obtenues pour les LSP http et vidéo sur demande. Les résultats sont indiqués pour le délai, la variation de délai dans une file d'attente, le taux de perte et l'utilisation. Les résultats sont en même temps discutés. Les séries en bleu représentent les résultats d'OPNET et celles en mauve, les résultats de la solution fondée sur l'algorithme AC-MVEv2.

4.3.1 Résultats des scénarios pour les délais des LSP

Les figures 4.3 et 4.4 affichent les délais moyens des LSP http obtenus pour les solutions concurrentes. Ils sont liés aux liaisons montante et descendante respectivement.

Pour ces niveaux modérés de congestion, les écarts de performance pour cette métrique sont peu significatifs entre les solutions. Les résultats sont tantôt identiques, tantôt légèrement différents. Lorsqu'ils sont dissemblables, les gains sont toujours supérieurs aux pertes. Il faut aussi remarquer l'augmentation du délai moyen avec celle du facteur d'augmentation de trafic.

Les figures 4.5 et 4.6 affichent les délais moyens des LSP vidéo sur demande en fonction du facteur d'augmentation de trafic. En matière de délai, les solutions concurrentes donnent des résultats similaires pour les LSP vidéo sur demande. Ainsi, notre proposition semble se comporter aussi bien que celle d'OPNET lorsque les

niveaux de congestion sont raisonnables pour ces LSP. Le délai moyen augmente avec le facteur d'augmentation de trafic.

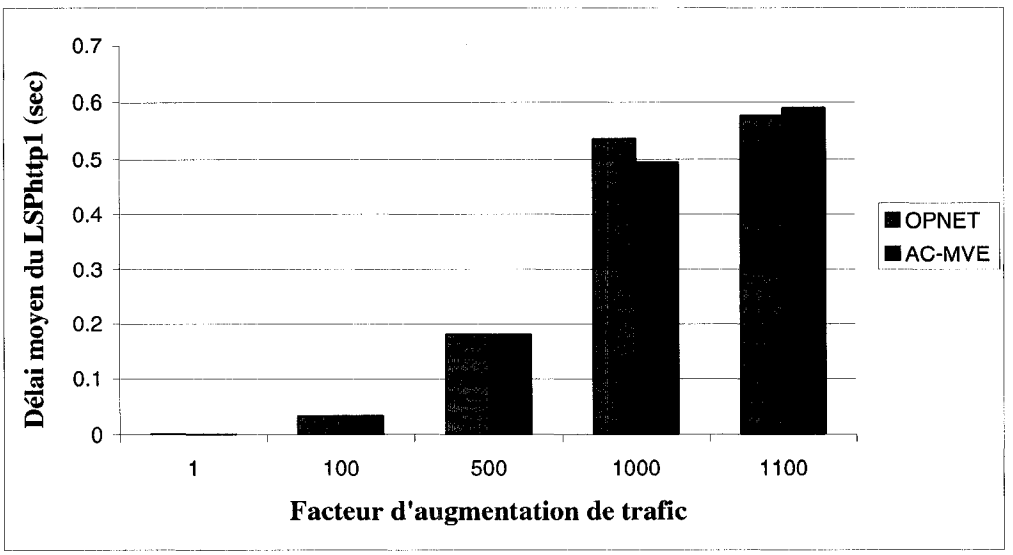

Figure 4.3 Délai moyen de LSPhttp1 versus le facteur d'augmentation de trafic

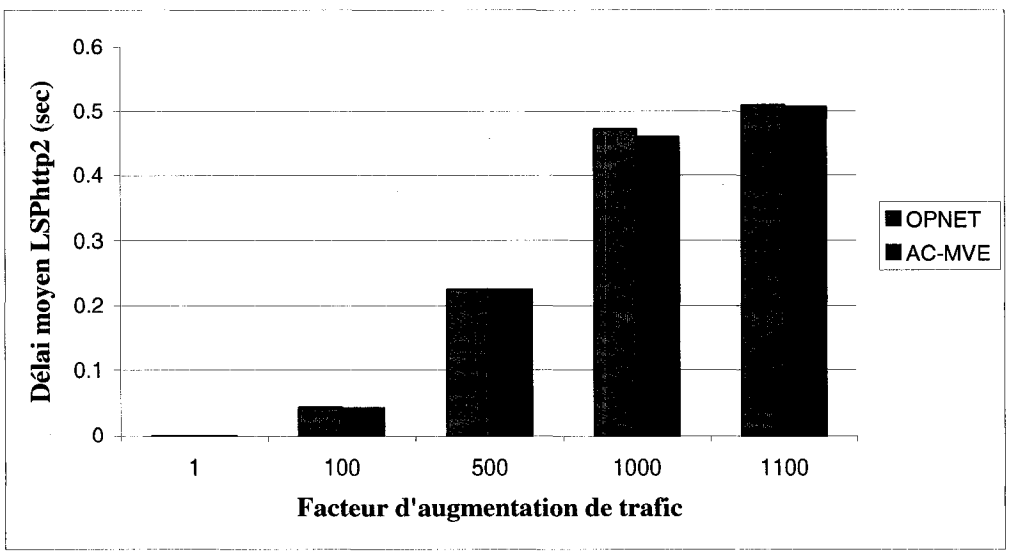

Figure 4.4 Délai moyen de LSPhttp2 versus le facteur d'augmentation de trafic

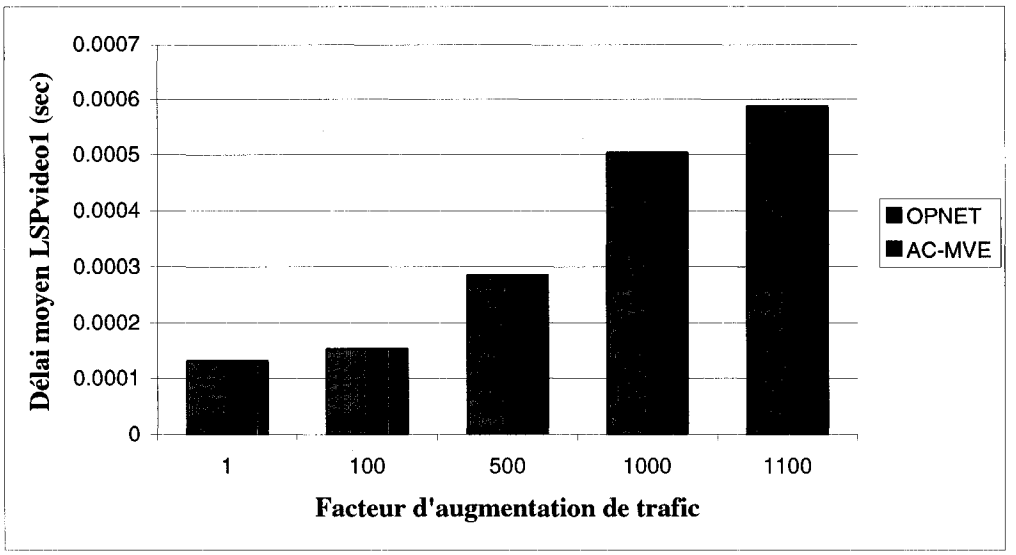

Figure 4.5 Délai moyen de LSPvideo1 versus le facteur d'augmentation de trafic

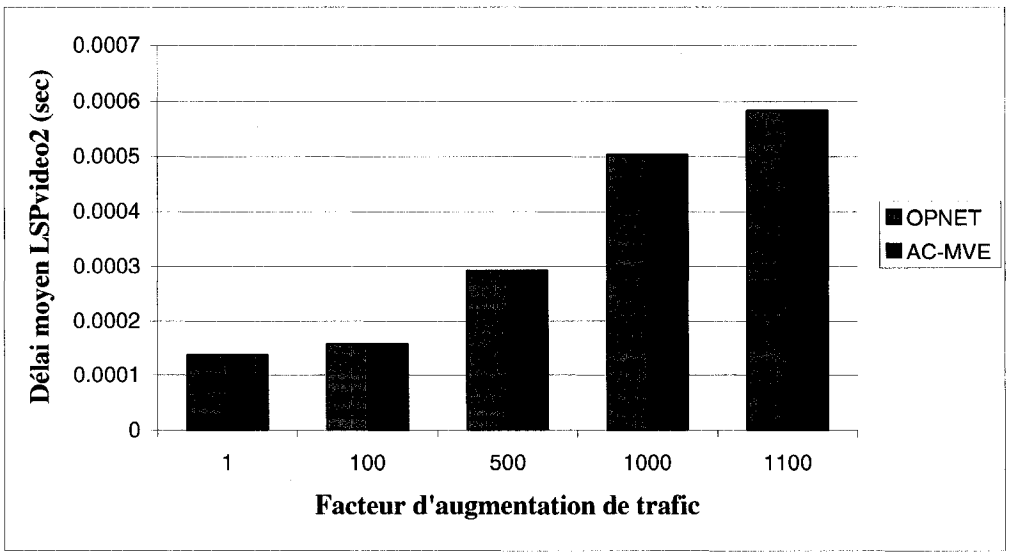

Figure 4.6 Délai moyen de LSPvideo2 versus le facteur d'augmentation de trafic

Pour la métrique du délai moyen, les solutions donnent des résultats différents uniquement pour les LSP de type http.

4.3.2 Résultats des scénarios pour les variations de délai des files d'attente des LSP

Les figures 4.7 et 4.8 affichent les variations moyennes pour le délai des files d'attente. Les files examinées sont associées aux interfaces des LSP http qui émanent des nœuds LER du domaine. Les figures révèlent un écart de performance entre les deux solutions. Les variations associées à celle fondée sur le mécanisme AC-MVEv2 sont généralement inférieures à celles d'OPNET, mais elles lui sont supérieures lorsque le facteur d'augmentation de trafic égale 1100. Mais, le plus grand écart est, pour les deux LSP, un gain de performance en faveur de notre solution. En outre, la variation de délai augmente avec le facteur d'augmentation de trafic, excepté une anomalie pour LSPhttp1 au facteur 1000.

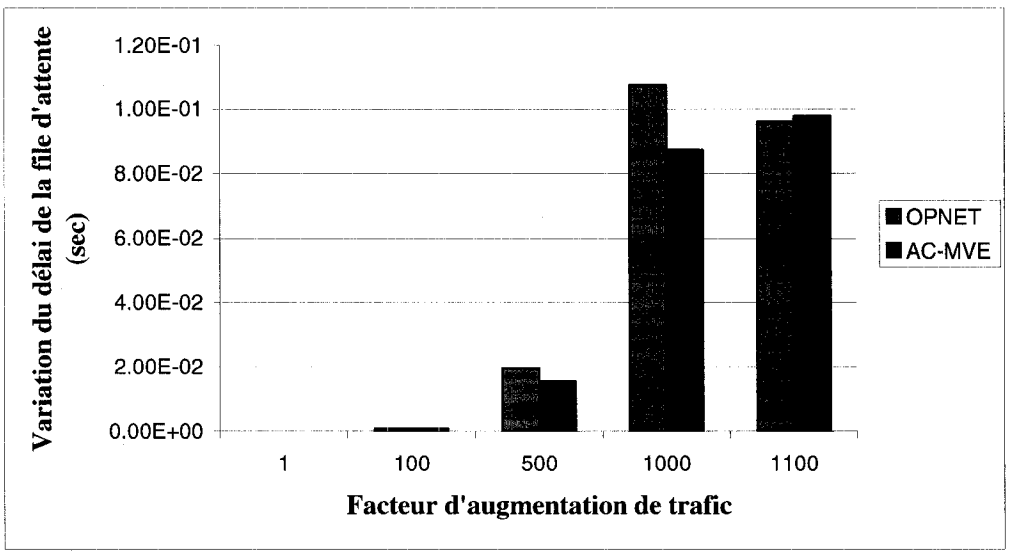

Figure 4.7 Variation moyenne du délai de la file d'attente pour l'interface du LER d'entrée de LSPhttp1 versus le facteur d'augmentation de trafic

Dans les figures 4.9 et 4.10, sont illustrées les variations moyennes des files d'attente pour les LSP vidéo sur demande. Les files sont liées aux interfaces des LSP vidéo qui émanent des nœuds LER du domaine.

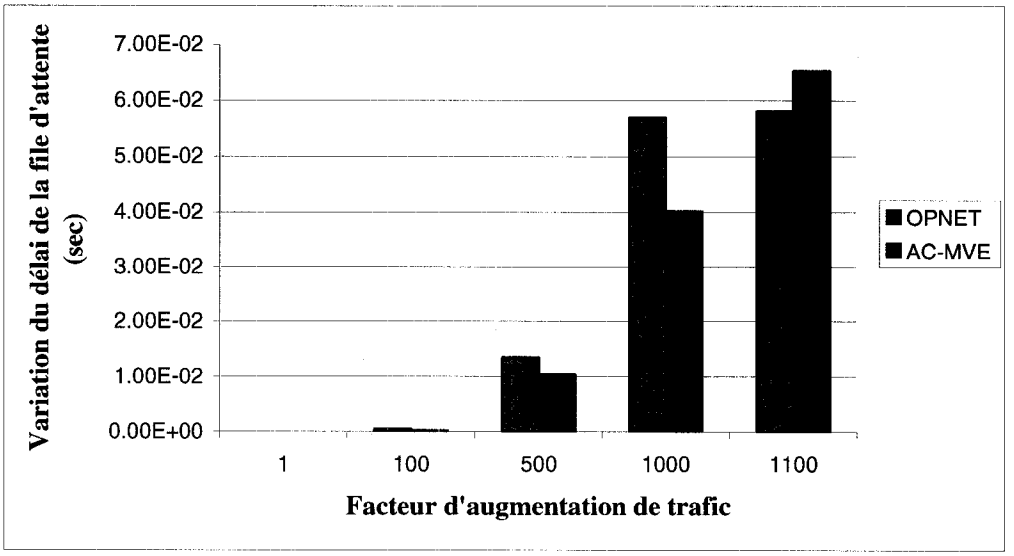

Figure 4.8 Variation moyenne du délai de la file d'attente pour l'interface du LER d'entrée de LSPhttp2 versus le facteur d'augmentation de trafic

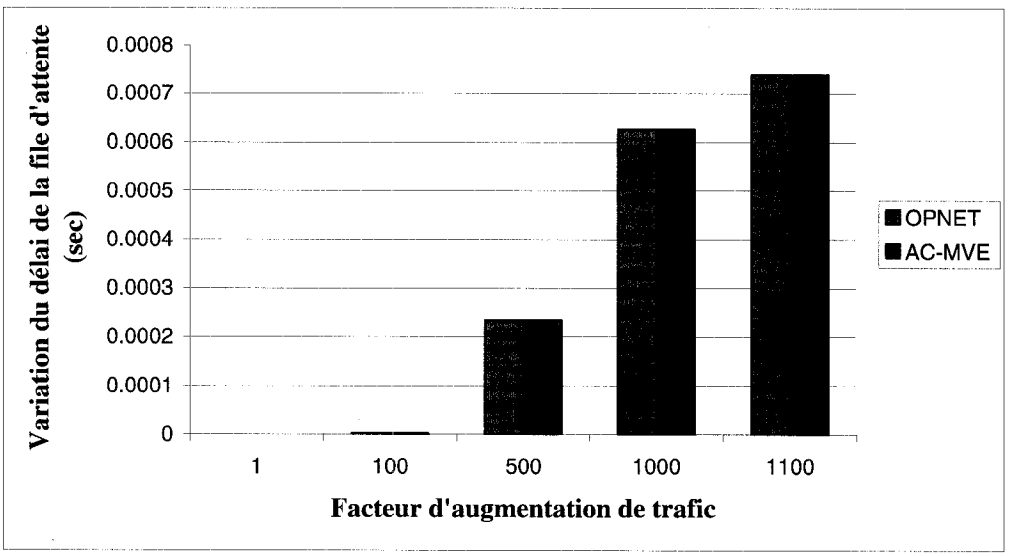

Figure 4.9 Variation moyenne du délai de la file d'attente pour l'interface du LER d'entrée de LSPvideo1 versus le facteur d'augmentation de trafic

Les solutions donnent des résultats similaires. Ainsi, la solution suggérée n'apporte aucun gain de performance par rapport à la solution d'OPNET lorsque les

niveaux de congestion sont modérés. La variation de délai augmente aussi avec le facteur d'augmentation de trafic.

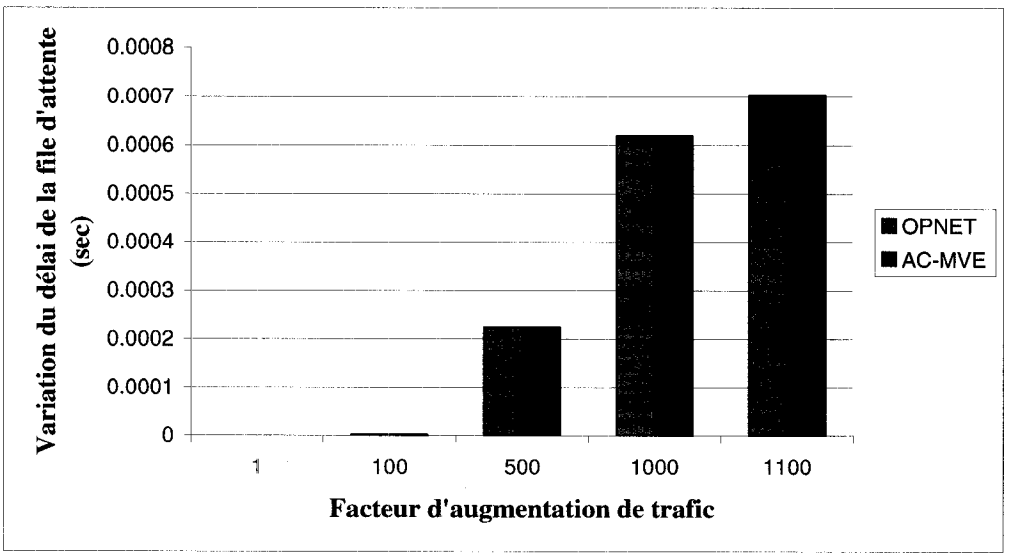

Figure 4.10 Variation moyenne du délai de la file d'attente pour l'interface du LER d'entrée de LSPvideo2 versus le facteur d'augmentation de trafic

4.3.3 Résultats des scénarios pour les taux de perte des LSP

Les figures 4.11 et 4.12 montrent les taux de perte des LSP http obtenus pour les solutions concurrentes. Ils sont liés aux liaisons montante et descendante respectivement.

Le taux de perte constitue sans doute la métrique qui affiche les plus grands écarts de performance entre les solutions comparées. Pour les LSP http, les taux de notre proposition sont généralement inférieurs à ceux d'OPNET. Cependant, à l'occasion, ils leur sont identiques ou supérieurs. Quoi qu'il en soit, les gains de performance observés pour notre solution sont nettement supérieurs aux pertes. De surcroît, ces pertes occasionnelles sont infimes comparativement aux gains. Notons le gain de performance particulièrement important du LSPhttp1 au facteur d'augmentation 1100. Ces résultats se rapportent à des scénarios qui sont caractérisés par des niveaux de

congestion modérés. Les taux de perte obtenus sont encourageants, car cet indicateur de qualité de service revêt une importance considérable pour les LSP de type http.

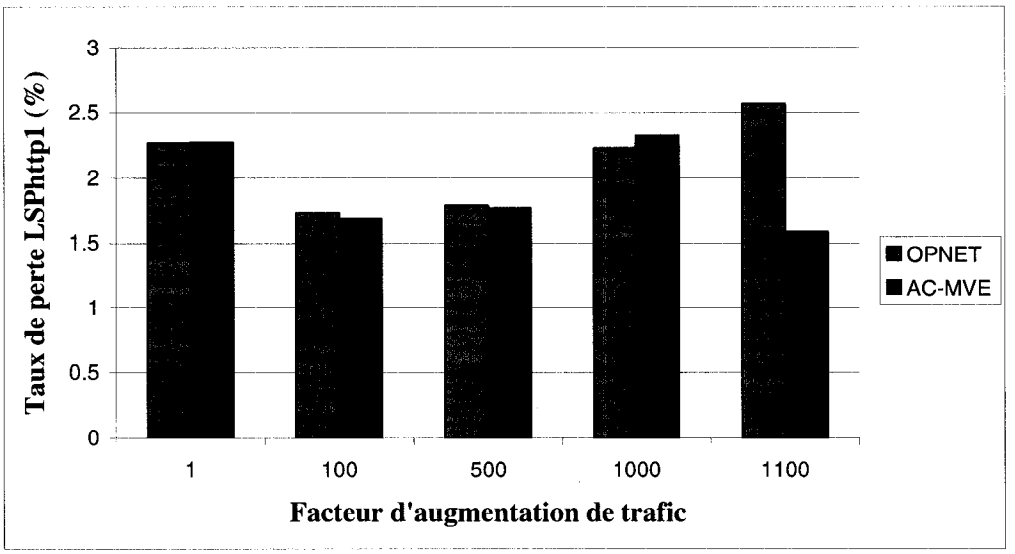

Figure 4.11 Taux de perte de LSPhttp1 versus le facteur d'augmentation de trafic

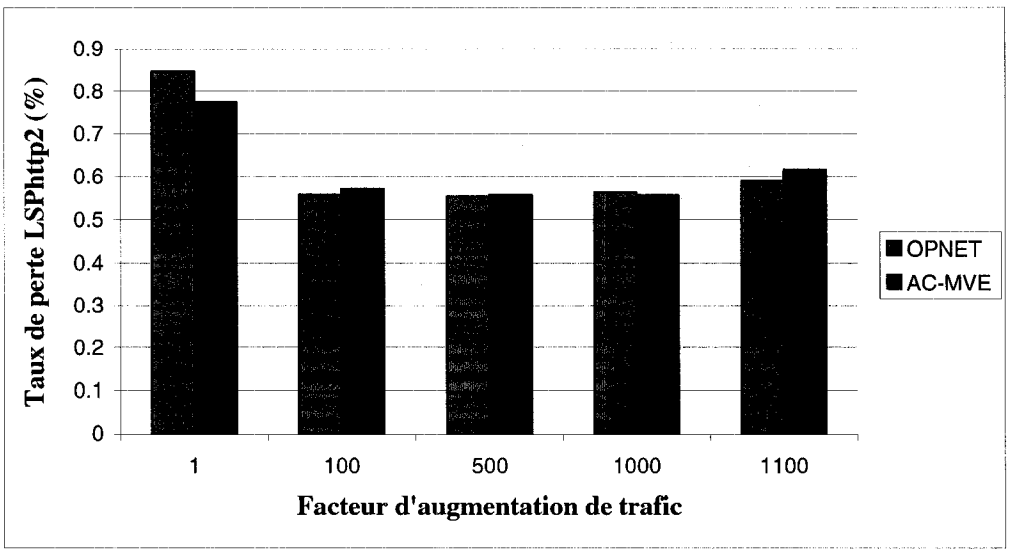

Figure 4.12 Taux de perte de LSPhttp2 versus le facteur d'augmentation de trafic

Les figures 4.13 et 4.14 montrent les taux de perte des LSP vidéo sur demande.

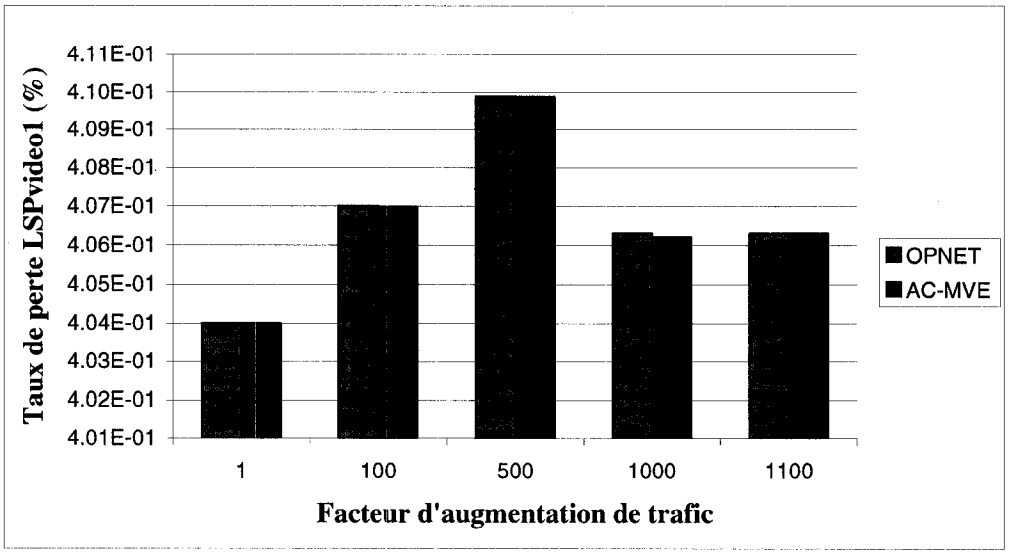

Figure 4.13 Taux de perte de LSPvideo1 versus le facteur d'augmentation de trafic

Contrairement aux résultats des LSP http, les valeurs pour les taux de perte des LSP vidéo sur demande sont généralement similaires lorsque les niveaux de congestion sont raisonnables. Toutefois, la solution suggérée conduit à une augmentation importante du taux de perte pour le LSPvideo2.

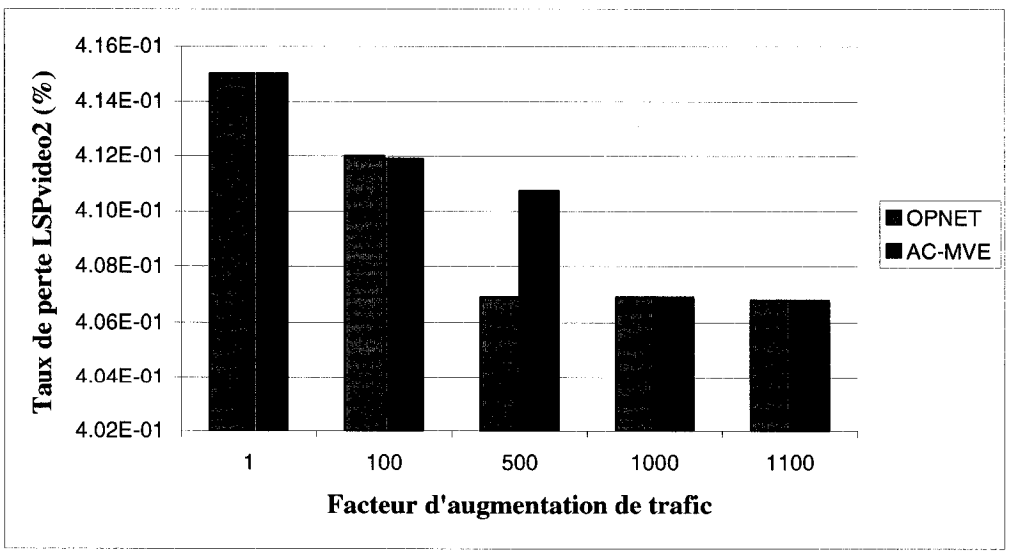

Figure 4.14 Taux de perte de LSPvideo2 versus le facteur d'augmentation de trafic

Pour le trafic de type vidéo sur demande, il ressort que les métriques délai et gigue sont privilégiées sur celle de taux de perte. En conséquence, les résultats obtenus sont dans l'ensemble acceptables. Néanmoins, l'augmentation constatée représente une anomalie. Elle sera donc expliquée plus tard.

4.3.4 Résultats des scénarios pour les utilisations des LSP

Les figures 4.15 et 4.16 indiquent les utilisations des LSP http qui ont été obtenues pour les solutions concurrentes. Les résultats sont donnés pour les liaisons montante et descendante respectivement. La solution fondée sur l'algorithme AC-MVEv2 donne généralement lieu à une légère sous-utilisation des liens des LSP de type http. Sinon, les résultats sont similaires. Si un gain de performance est constaté, il est infinitésimal.

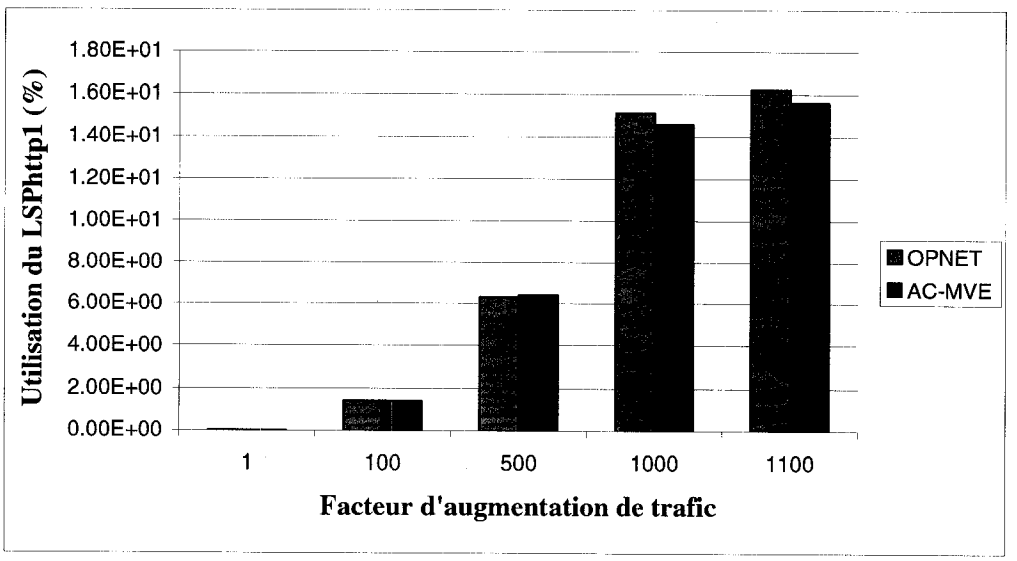

Figure 4.15 Utilisation moyenne de LSPhttp1 versus l'augmentation de trafic

Les figures 4.17 et 4.18 donnent les utilisations obtenues pour les LSP vidéo sur demande.

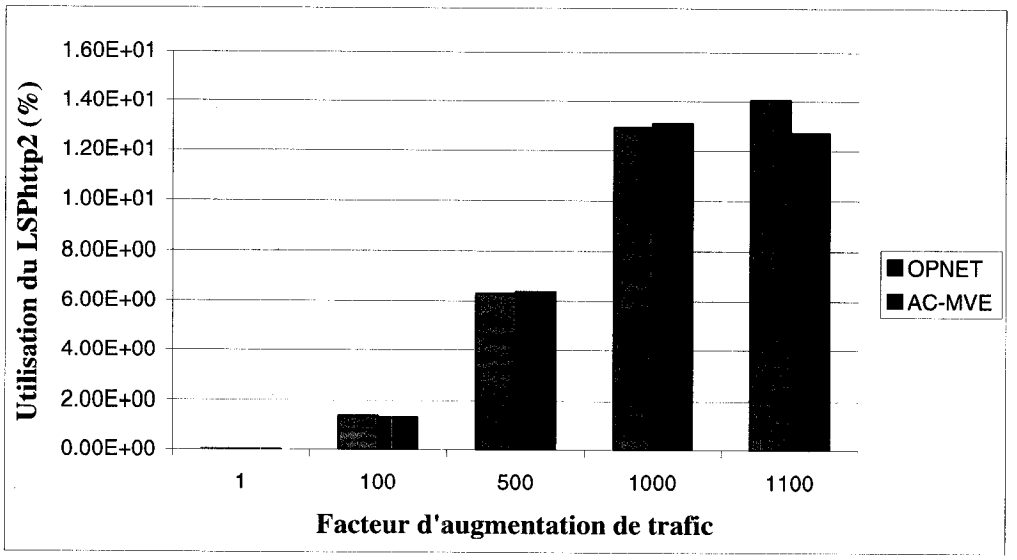

Figure 4.16 Utilisation moyenne de LSPhttp2 versus l'augmentation de trafic

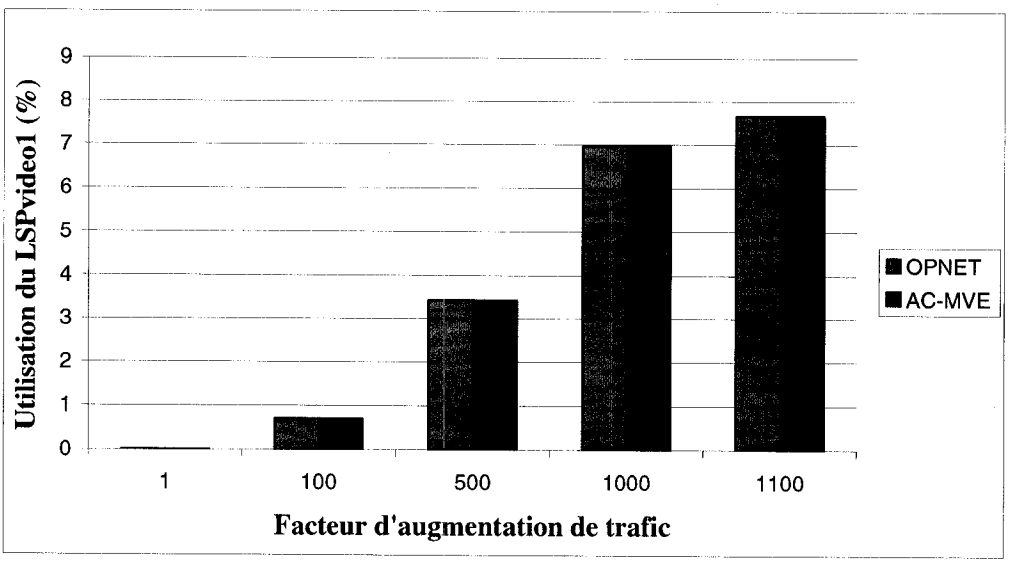

Figure 4.17 Utilisation moyenne de LSPvideo1 versus l'augmentation de trafic

Les résultats sont similaires pour les LSP de type vidéo sur demande lorsque les niveaux de congestion sont modérés. Nous remarquons que des écarts de performance peuvent être observés même lorsque l'utilisation du LSP est petite. Ceci est conforme aux résultats des études pour les sources utilisant UDP, c'est-à-dire que le

dimensionnement des liens doit être exagéré pour assurer une performance acceptable du système lorsque le trafic convoyé possède les propriétés d'auto-similarité et de dépendance à long terme.

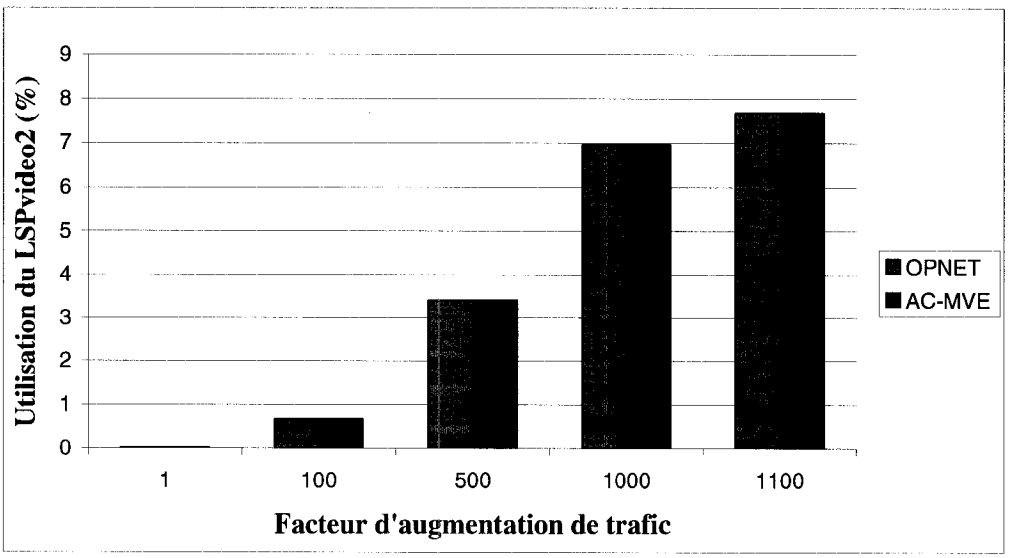

Figure 4.18 Utilisation moyenne de LSPvideo2 versus l'augmentation de trafic

En somme, la solution basée sur AC-MVEv2 fournit des résultats acceptables, quelques anomalies exceptées. Les résultats, toutefois, se rapportent à des scénarios caractérisés par des niveaux de congestion modérés. Aussi, la contribution de l'algorithme n'est pas vraiment appréciée avec cette évaluation de performance, mais il ne pouvait en être autrement en raison des lacunes d'OPNET et des artifices d'implémentation réalisés pour les pallier. Ces artifices incluent celui qui consiste à rejeter systématiquement les paquets associés aux flots refusés et celui qui consiste à fournir une dynamique des arrivées et départs des flots à l'algorithme de contrôle d'admission. Les anomalies découlent, d'une part, des adaptations au code et à l'environnement de simulation et, d'autre part, des incohérences soupçonnées dans le code d'OPNET. En ce qui a trait aux conséquences des adaptations pour le code, citons les réactions des protocoles adaptatifs à l'état du réseau, particulièrement celles des

émetteurs TCP devant les pertes des paquets des flots refusés. Ces pertes ne devraient pas être perçues, car, dans la réalité, les paquets ne sont pas générés pour les flots refusés. Les détails relatifs à ces adaptations sont donnés aussitôt après.

Par ailleurs, les expériences montrent que le compromis entre la qualité de service et l'utilisation des ressources est remis en cause par notre solution lorsque le trafic d'un LSP présente des fluctuations importantes et surtout lorsque ces fluctuations peuvent difficilement être contenues par les liens des LSP affectés au trafic. En particulier, le rapport débit maximum/débit moyen de LSPhttp1 égale 15521 tandis que celui de LSPvideo1 égale 45.8. En conséquence, le degré d'auto-similarité des LSPhttp est sans doute supérieur à celui des LSP vidéo sur demande. Avec cette remarque, nous expliquons en partie les écarts de performance souvent nuls des LSP vidéo sur demande et les valeurs plus « versatiles » de ces écarts pour les LSP http. Cette constatation trahit les efforts déployés par l'algorithme pour contrer les propriétés excentriques du trafic. En l'absence de ces composantes dans le trafic, l'algorithme peut donc donner des résultats similaires à ceux d'une solution dépourvue de mécanisme de contrôle d'admission lorsque les niveaux de congestion sont modérés.

Enfin, si les résultats accusent une certaine instabilité du système, ils révèlent l'incontournable nécessité de déployer des modules de conditionnement efficaces et conscients de la présence des composantes d'auto-similarité et de dépendance à long terme dans le trafic. Plus généralement, les algorithmes de contrôle de congestion et les codecs doivent tout faire pour adoucir le trafic et diminuer autant que possible ses rafales. En effet, un mécanisme de contrôle d'admission agit uniquement sur réception d'une requête. Il est moins actif que les autres modules, particulièrement ceux qui s'exécutent à des échelles de temps inférieures, tels que ceux pour la gestion du tampon, l'ordonnancement et la mise en forme (*shaping*).

4.4 Analyse globale et mérite de la solution

Le réseau de base considéré constitue une représentation de la solution fondée sur l'algorithme AC-MVEv2. En dépit des adaptations liées au code et à

l'environnement de simulation, l'évaluation de performance révèle des informations utiles susceptibles de raffiner la solution globale relativement à son volet de « disponibilité des ressources ». Dans cette section, la solution globale et la preuve de concept sont analysées et critiquées. Le mérite de la solution proposée est ensuite démontré.

Analyse globale

Pour le volet « disponibilité des ressources », les résultats sont acceptables, à quelques anomalies près. Les constatations s'appliquent lorsque les niveaux de congestion sont modérés. Ci-après, les résultats et les anomalies sont commentés et ensuite expliqués par les facteurs limitatifs de la preuve de concept.

Somme toute, notre solution ne se démarque pas de manière extraordinaire avec notre preuve de concept. Les gains timides de performance et les anomalies sont directement liés aux adaptations relatives au code et à l'environnement de simulation. Les résultats découlent des adaptations adoptées pour effectuer la preuve de concept et remédier aux incohérences répertoriées dans OPNET - et à celles soupçonnées. L'adaptation mère des autres artifices est sans doute celle d'employer un réseau non UMTS et uniquement basé sur les technologies MPLS et DiffServ. En conséquence, les sources n'envoient pas de requêtes d'activation/modification de contexte PDP de sorte que les nœuds LER ne reçoivent pas de requêtes devant conduire à une exécution de l'algorithme de contrôle d'admission.

En plus d'être incapable de distinguer les paquets des nouveaux flots de ceux des anciens, l'algorithme n'est pas au courant des flots qui quittent le système. En conséquence, un premier artifice d'implémentation est réalisé pour fournir à l'algorithme une certaine connaissance de la dynamique des arrivées et départs des flots du système. En outre, une requête refusée n'empêche pas la source génératrice de la requête d'entamer la phase de transmission des paquets : elle indique au nœud d'entrée/sortie LER qui héberge les processus d'intérêt de discriminer les paquets qui correspondent à

la requête refusée et de les rejeter systématiquement. Cette astuce est le second artifice d'implémentation qui porte préjudice à notre évaluation de performance.

Ainsi, la preuve de concept est affectée par les artifices susmentionnés. Effectivement, les sources génèrent des paquets pour des flots refusés, des paquets qui ne seraient pas générés en réalité – une réponse négative à une requête d'activation/modification de contexte PDP informerait ces sources de ne pas entamer la phase de transmission des paquets. Donc, les sources continuent à transmettre et c'est le nœud périphérique LER qui rejette les paquets associés aux requêtes refusées. En conséquence, les protocoles adaptatifs peuvent essayer de recouvrer la stabilité à des périodes où le système ne se trouve pas dans un état de congestion, mais dans un état de congestion illusoire, créé par l'algorithme lui-même.

Particulièrement, les émetteurs TCP peuvent percevoir de fausses pertes et donc continuer à traverser les différentes phases de contrôle de congestion. La version Reno du protocole TCP est employée dans OPNET. Les phases sont donc : *slow-start*, *congestion avoidance*, *fast recovery/fast retransmit* et *exponential backoff*. Lors de son séjour dans ces phases, l'émetteur TCP adapte son débit afin de combattre la congestion. Ainsi, les métriques délai, taux de perte, gigue et utilisation sont affectées par les interactions de ce protocole avec le réseau. En conséquence, nous pensons que nos résultats sont dus au caractère chaotique du protocole et qu'il est donc superflu d'essayer de trouver des tendances et d'expliquer de plus près les relations observées entre les résultats pour le débit, le taux de perte et l'utilisation de notre solution. Il faut toutefois noter la sensibilité toute particulière du taux de perte par rapport à celle des autres métriques.

Outre les effets subversifs de ces artifices d'implémentation, il est important de souligner les conséquences des adaptations relatives à l'environnement de simulation. La première d'entre elles a trait aux modules de conditionnement employés, particulièrement à la nature des profils de QdS adoptés. Afin qu'ils ne dénaturent pas le trafic et ne mettent pas en forme son auto-similarité et sa dépendance à long terme, ils sont permissifs. Mais, de tels profils sont irréalistes et ne contribuent pas à limiter les

fluctuations du trafic. Par ailleurs, les paramètres WFQ défavorisent énormément le trafic http, car ils fournissent à celui-ci un poids de 30 et au trafic vidéo sur demande un poids de 70. Enfin, les tailles pour les files d'attente et les tampons sont peu réalistes. Elles devraient être inférieures pour le trafic vidéo sur demande. Cependant, les résultats doivent être évalués de manière relative.

Pour ainsi dire, les adaptations réalisées expliquent la performance de la solution proposée. Néanmoins, elle donne des résultats acceptables. La preuve de concept pour le volet « disponibilité des ressources » est donc réalisée sur une représentation de la solution non sans fautes. Le réseau employé n'est pas un réseau UMTS de la version 5. Son architecture, sa topologie, ses protocoles et sa charge sont largement simplifiés. Les éléments limitatifs de cette preuve de concept sont importants. Elle n'intègre pas la mobilité et n'inclut pas l'infrastructure radio. Elle abstrait la signalisation des requêtes de contexte PDP et les échanges SNMP. Elle n'implémente pas le module AC-KQv2 et ne calibre pas le mécanisme AC-MVEv2 (et les algorithmes ne sont pas comparés). Elle ne fournit pas de réponse quant à la correction double apportée au paramètre α de l'algorithme AC-MVEv2. En effet, il aurait été intéressant de comparer la performance de l'algorithme dans deux cas. Dans le premier, la correction pour l'erreur d'échantillonnage est simple et apportée sur une valeur fixe; dans le second, elle est double et apportée sur une valeur variable qui s'adapte au réseau (notre solution actuelle). Les paramètres WFQ, les tailles pour les files d'attente et les tampons doivent aussi être ajustés. De plus, les mécanismes d'inter-fonctionnement entre les technologies UMTS, MPLS et DiffServ (mises en correspondance, etc.) ne sont pas implémentés; or, certains vices de fonctionnement peuvent résulter simplement des défauts d'interopérabilité. Noter que le *Bandwidth Broker* n'est pas implémenté.

En outre, la preuve de concept est aussi limitée par le fait que le volet « politique » ne soit pas implémenté. Autrement dit, la mécanique relative à cet aspect du schéma de fonctionnement est complètement abstraite, car les serveurs et les clients qui concourent à la gestion basée sur des politiques sont absents du modèle. Pourtant, le volet « disponibilité des ressources » est conditionné par le volet « politique »,

particulièrement parce que les processus d'acquisition des mesures et d'analyse doivent se soumettre aux politiques de l'opérateur. En effet, il influence notamment la survivabilité et la stabilité du système. Entre autres, la mise à jour des paramètres des tables FTN et ILM ainsi que la modification des LSP ne sont pas réalisées. En fait, les expériences évaluent le fonctionnement du volet « disponibilité des ressources » lorsque les éléments précités sont figés. Dans notre représentation, les procédures spécifiques à la gestion basée sur des politiques (SIP, COPS, etc.) ne sont pas implémentées.

De toute façon, certains éléments de notre solution ne sont pas explicités et plusieurs détails ne sont pas fournis dans le cadre générique de 3GPP. Parmi les données manquantes ou à être explicitées, citons les conditions et les actions de configuration des politiques, les objets des modules PIB et MIB ainsi que les règles des mises en correspondance SDP-politiques, SDP-DiffServ-UMTS, PIB-MIB, etc. Il faut aussi ajouter à cette liste les différents niveaux de QdS (du ressort de l'opérateur) et l'organigramme complet du schéma de fonctionnement global (*flowchart*), depuis l'usager d'origine jusqu'à la destination et en passant par toutes les entités concernées. D'autres détails sont aussi importants, tels que la parallélisation des opérations et la mise en cache.

Enfin, l'opérateur et l'instance 3GPP doivent expliciter certains détails. Nous devons aussi éclaircir certaines questions. Il sera par la suite possible de définir les volets « politique » et « disponibilité de ressources » de la solution proposée, laquelle peut faire emploi de l'algorithme AC-MVEv2 ou de l'algorithme AC-MVEv2. Les mécanismes de conditionnement doivent être bien choisis. Après, il sera possible d'exécuter des expériences de simulation fidèles à la réalité, c'est-à-dire sur un réseau UMTS de la version 5 qui supporte les technologies MPLS, DiffServ et SNMP. Le délai de réponse et les indicateurs de stabilité, d'évolutivité et de survivabilité permettront d'évaluer la viabilité de solution.

Mérite de la solution

Après cette revue sommaire des effets des adaptations au code et à l'environnement de simulation, il apparaît nécessaire de situer la solution proposée. Ci-après, le mérite de celle-ci est démontré.

Si l'évaluation de performance fournit des informations utiles, elle ne parvient pas à situer correctement la solution suggérée. Elle donne cependant des résultats encourageants. Un examen rapide de la proposition permet de montrer certains de ses avantages et inconvénients. Entre autres, intuitivement, nous pouvons penser qu'elle peut apporter un gain de performance pour le délai, le taux de perte et la gigue. Toutefois, par compensation, elle peut donner lieu à une diminution de l'utilisation des ressources et coûter cher en ressources financières et effort humain préalable, lequel effort humain peut s'avérer appréciable pour le dimensionnement des LSP et la rédaction des politiques.

Malgré son immaturité, la solution mérite d'être approfondie, car elle est tout à fait avant-gardiste par rapport à celles vues dans la littérature. En effet, elle définit le volet « disponibilité des ressources » et apporte des modifications au volet « politique ». Ainsi, elle enrichit à la fois le schéma de fonctionnement global et le processus de contrôle d'admission qui est propre au domaine à commutation de paquets du réseau de cœur. En outre, elle améliore le degré de coopération entre les volets précités pour le bien du système d'ingénierie de trafic global. Elle se présente aussi comme une solution ébauche qui offre un compromis tout autre entre l'utilisation des ressources et la qualité de service. À titre de rappel, le compromis traditionnel était fortement biaisé en faveur de la première contrainte, ce qui est inacceptable pour les services et applications sophistiqués prévus par les opérateurs des réseaux UMTS de la version 5.

Enfin, la proposition peut constituer une borne pour les solutions ultérieures, aussi grossière puisse t-elle s'avérer. Elle peut aussi être raffinée et améliorée au fur et à mesure, car il est possible d'ôter certaines de ses composantes coûteuses en performance ou encore de les modifier.

CHAPITRE 5
CONCLUSION

À la cinquième version de normalisation d'UMTS, un schéma de gestion basé sur des politiques est adopté. Il est fondé sur le sous-système multimédia IMS, une extension au domaine à commutation de paquets du réseau de cœur. Un mécanisme de contrôle d'admission basé sur des politiques est également développé, celui-ci reposant sur les politiques de l'opérateur et les ressources disponibles dans le réseau. Dans le but d'améliorer le cadre générique de 3GPP, un schéma de fonctionnement basé sur des politiques est suggéré. Il bénéficie d'une connaissance réelle de la disponibilité des ressources et se dote d'un mécanisme de contrôle d'admission basé sur des politiques et des mesures. Ce dernier chapitre présente une synthèse des travaux, les limitations principales de l'étude et quelques indications pour des recherches futures.

5.1 Synthèse des travaux

Une lecture attentive des documents de la littérature permet de déceler, au sein des volets politique et disponibilité des ressources, plusieurs éléments sujets à améliorations. En dépit de l'importance du second volet dans la gestion des ressources et malgré les propriétés excentriques du trafic des réseaux 3G, ce volet est peu traité dans le cadre générique de l'instance d'UMTS. Mais, le volet politique est aussi imparfait. Par exemple, le seul nœud tenu d'être un client de politiques est la passerelle GGSN. De plus, les politiques définies sont peu variées. Donc, ce mémoire suggère un algorithme de contrôle d'admission et un schéma de fonctionnement global; les deux reposent sur des politiques et des mesures.

À la lumière de l'ensemble des constatations, nous avons proposé un schéma de fonctionnement et un mécanisme de contrôle d'admission qui s'appuient sur des politiques et des mesures. Les caractéristiques de la solution globale sont tirées de la vaste littérature et des cadres génériques des instances IETF et 3GPP. Les modifications

visent à enrichir la gestion basée sur des politiques avec la connaissance de la disponibilité des ressources. Des mécanismes de contrôle d'admission basés sur des mesures sont employés parce que ceux-ci sont mis de l'avant par les études [3, 24]. Ils peuvent pallier les propriétés excentriques dans le trafic et les changements qui se produisent dans les réseaux de troisième génération.

Dans la solution globale, nous suggérons l'addition de fonctionnalités et de mécanismes à certains éléments du réseau ainsi que la modification des processus d'établissement de session pour l'ensemble des services sophistiqués. Il peut en découler –de ces changements- un degré supérieur d'automatisme pour le schéma de gestion et, conséquemment, une amélioration de la qualité de service. Nous préconisons des politiques plus variées et définissons le sous-système pour les services élaborés EISS (*Enhanced IP Services Subsystem*). Ce successeur du sous-système multimédia IMS concourt à la gestion basée sur des politiques pour les contrats de haut niveau de qualité de service. Le schéma de fonctionnement repose sur des LSP pseudo-statiques de type L-LSP, un SGSN abritant un client de politiques, un *Bandwidth Broker* hébergeant le mécanisme de contrôle d'admission AC-MVEv2/AC-KQv2 et des entités SNMP dédiées à l'acquisition des mesures d'utilisation des LSP. Le *Bandwith Broker* possède une connaissance globale de la disponibilité des ressources. Il faut noter que le paramètre α de l'algorithme AC-MVEv2 n'a pas à être choisi au préalable à l'aide de simulations. De plus, il varie avec l'état du réseau. Les deux algorithmes ont été retenus parce qu'ils sont simples et fondés sur des hypothèses moins fortes que celles de leurs concurrents trouvés dans la littérature.

En ce qui concerne l'évaluation de performance, elle a uniquement porté sur le volet disponibilité des ressources. La preuve de concept a été effectuée sur un réseau non UMTS supportant les technologies MPLS et DiffServ. Ensuite, seul l'algorithme AC-MVEv2 a été implémenté. Les résultats obtenus sont acceptables, quelques anomalies exceptées. Ils se rapportent, toutefois, à des scénarios caractérisés par des niveaux de congestion modérés. Aussi, la contribution de l'algorithme AC-MVEv2 n'est pas vraiment appréciée avec cette évaluation de performance, mais il ne pouvait en

être autrement en raison des lacunes d'OPNET et des artifices d'implémentation réalisés pour les pallier. Les anomalies découlent, d'une part, des adaptations au code et à l'environnement de simulation et, d'autre part, des incohérences soupçonnées dans le code d'OPNET.

Quoi qu'il en soit, l'évaluation de performance effectuée a révélé les contributions des protocoles adaptatifs aux composantes d'auto-similarité et de dépendance à long terme du trafic (particulièrement de TCP). De plus, en plus d'avoir souligné l'importance des paramètres WFQ et celle des tailles pour les tampons et les files d'attente, elle a montré combien un module de contrôle d'admission peut s'avérer inapte à combattre la congestion sans l'aide de mécanismes de contrôle de congestion complémentaires efficaces. De manière générale, il est impératif de concevoir des mécanismes de conditionnement efficaces et, particulièrement, d'améliorer le protocole TCP pour le rendre moins chaotique. L'amélioration de TCP fait d'ailleurs l'objet de recherches à l'IETF [17].

5.2 Limitations principales

Ce mémoire propose des solutions intéressantes susceptibles d'améliorer la gestion basée sur des politiques de 3GPP. Cependant, certains problèmes sont laissés pour compte. Cette section énumère les limitations relatives à notre recherche et à notre implémentation.

En ce qui concerne la preuve de concept, elle comporte des limitations en raison des hypothèses et des adaptations reliées au code et à l'environnement de simulation. Entre autres choses, le réseau employé et la charge sont peu représentatifs de la réalité. Le modèle utilise des valeurs irréalistes pour les paramètres WFQ, les profils, la taille des tampons et celle des files d'attente. Les paramètres ne sont pas adaptés à la nature de la classe. Par exemple, les tailles associées au trafic vidéo sur demande devraient être inférieures à celles associées au trafic http. Ensuite, le modèle comporte un petit nombre de sources de trafic et chaque source génératrice de requêtes ne supporte qu'une seule application.

Toutefois, les limitations principales de la preuve de concept sont liées à la version du logiciel employée. Elle comporte des erreurs et des incohérences dans le code d'UMTS. Donc, le modèle utilise DiffServ et repose sur des L-LSP statiques qui sont disjoints pour les liaisons montante et descendante du trafic http. Ceci permet d'éviter les sections louches du code MPLS, notamment celle qui entoure la réservation de bande passante pour un LSP statique. Le modèle permet également de ne pas utiliser le code d'UMTS, car celui-ci comprend des erreurs majeures qui ont été confirmées par le groupe de support d'OPNET. En conséquence, les effets de la mobilité ne sont pas connus et, donc, la relève et les requêtes de modification de contexte ne sont pas supportées. Le mécanisme de contrôle d'admission n'est pas exécuté suite à une mobilité ou, plus généralement, suite à une demande de modification des paramètres de la session. Le réseau n'étant pas de type UMTS, il ne véhicule pas de requêtes d'activation ou de modification de contexte PDP. De plus, comme les LSP ne sont pas dynamiques, l'algorithme ne peut pas repérer les nouveaux flots, car des requêtes ne sont pas effectivement signalées par l'usager (RSVP, LDP, etc.). Ensuite, les effets de la congestion entre les classes ne sont pas connus, même ceux au niveau d'un nœud LER.

Afin de remédier aux problèmes dans OPNET aussi simplement que possible, deux artifices d'implémentation sont réalisés. Ces artifices incluent celui qui consiste à rejeter systématiquement les paquets associés aux flots refusés et celui qui consiste à fournir une dynamique des arrivées et départs des flots à l'algorithme de contrôle d'admission. À cause du second artifice, les expériences de simulation considèrent des niveaux de congestion modérés. En outre, les profils de QdS, les mécanismes de conditionnement et les paramètres de configuration du réseau (WFQ, file d'attente, tampon, etc.) ne sont pas réalistes et affectent certainement l'évaluation de performance. Par ailleurs, les métriques utilisées dans l'évaluation de performance sont insuffisantes, car elles devraient permettre d'indiquer – autant que faire se peut - comment la solution satisfait les recommandations pour les systèmes d'ingénierie de trafic (stabilité, évolutivité, survivabilité, etc.).

En ce qui a trait à la solution proposée, elle doit être détaillée, car elle se trouve au stade d'ébauche. Certains aspects ne sont pas précisés, plusieurs doivent être améliorés et d'autres ne sont pas touchés. Ces remarques s'appliquent autant pour le volet politique que pour le volet disponibilité des ressources. Entre autres, des mécanismes de conditionnement efficaces ne sont pas suggérés. De plus, les algorithmes AC-MVEv2 et AC-KQv2 ne sont pas calibrés, c'est-à-dire que les valeurs pour la période d'échantillonnage, la taille de la fenêtre des mesures et l'intervalle de confiance ne sont pas réglées. La correction appropriée pour l'intervalle de AC-MVEv2 n'est pas connue et la qualité des deux algorithmes est difficile à évaluer de sorte qu'il est impossible de fournir une recommandation. Ensuite, les valeurs des liens des LSP et la topologie des LSP ne sont pas déterminées. En outre, les niveaux de QdS ne sont pas spécifiés (ni le nombre de ces niveaux) et les conditions et actions de configuration relatives aux politiques ne sont pas développées. Les objets des modules MIB et PIB ne sont pas donnés et l'organigramme complet du schéma de fonctionnement global (*flowchart*) n'est pas décrit. Finalement, des détails divers, tels la parallélisation des opérations et la mise en cache, ne sont pas explicités. Mais, ces informations dépendent beaucoup de l'opérateur.

5.3 Indications pour des recherches futures

En raison des limitations de l'évaluation de performance et du mérite de la solution, il apparaît nécessaire de réaliser de nouvelles expériences de simulation. En effet, les volets reliés aux politiques et à la disponibilité des ressources amènent des avantages, mais aussi des inconvénients. De plus, la proposition offre un compromis particulier entre l'utilisation des ressources et la qualité de service. Une meilleure preuve de concept s'impose pour le volet évalué dans ce travail. Les nouvelles simulations doivent utiliser un réseau UMTS de la version 5. Celui-ci doit supporter les technologies MPLS, DiffServ et SNMP. La mobilité doit donc être prise en compte et les requêtes de modification de contexte doivent être supportées. Une comparaison sérieuse des algorithmes AC-MVEv2 et AC-KQv2 est aussi nécessaire et ils doivent être

calibrés. Il serait intéressant de simuler AC-MVEv2 et de justifier son emploi d'une correction double par rapport à celui d'une correction simple pour l'intervalle de confiance. Ceci permettrait de voir laquelle des corrections donne lieu à un algorithme plus conservateur ou instable. À titre de rappel, la correction simple est dérivée d'une valeur fixe, par opposition à la correction double qui manipule une valeur variable. Le meilleur des deux algorithmes pour notre schéma doit également être trouvé. Il serait intéressant de concevoir une méthode efficace pour dimensionner les liens et trouver une topologie adéquate des LSP. Le degré d'auto-similarité du trafic dans chaque LSP devrait aussi être mesuré, de même que les effets de la congestion entre les classes et à l'intérieur de celles-ci.

Mais, une évaluation de performance doit être réalisée pour la solution globale. Le volet politique doit donc être fixé. De toute façon, il influence celui de la disponibilité des ressources. Pour ce faire, des politiques doivent être articulées autour de conditions et d'actions de configuration cohérentes. Par exemple, certaines peuvent conduire à l'activation ou à la désactivation de composantes du système d'ingénierie de trafic, notamment faire basculer le mécanisme entre les modes actif et inactif. Certaines applications du système d'ingénierie de trafic à long terme fournissent d'ailleurs des patrons de trafic qui peuvent révéler des plages temporelles ou des événements durant lesquels la disponibilité des ressources devrait être évaluée pour répondre à une requête. Nous pouvons ainsi imaginer une politique conduisant à l'activation du mécanisme aussitôt qu'un taux seuil préalablement fixé est dépassé par le taux de perte mesuré sur un LSP. Les nouvelles politiques visent à améliorer le système d'ingénierie de trafic, c'est-à-dire ses sous-systèmes de mesure, de modélisation et d'analyse et d'optimisation. Par ailleurs, les éléments des bases PIB et MIB doivent être spécifiés et plusieurs éléments du système doivent être précisés, notamment ceux reliés à la mise en cache et à la parallélisation de certaines procédures. L'organigramme doit aussi être détaillé.

Finalement, l'évaluation de performance doit inclure une variété de métriques. Citons, à titre d'exemple, le délai de réponse et les indicateurs de performance pour la stabilité, la qualité de service, l'utilisation des ressources et l'évolutivité.

BIBLIOGRAPHIE

[1] SANCHEZ, J. et THIOUNE, M., *UMTS services, architecture et WCDMA*, Paris : Hermès Science, pp. 17-118, 2001.

[2] 3GPP Technical Specification Group Services and System Aspects, *QoS concept and architecture*, 3GPP TS 23.107 v5.8.0. (2003-03), 40 pages, 2003

[3] MOORE, A. W., *Measurement-Based Management of Network Resources*, Computer Laboratory Technical Report 528, Université de Cambridge, http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-528.pdf, pp. 7- 208, av. 2002.

[4] 3GPP Technical Specification Group Services and System Aspects, *End-to-End quality of service (QoS) concept and architecture*, 3GPP TS 23.207 v5.8.0 (2003-06), 47 pages, 2003.

[5] 3GPP Technical Specification Group Services and System Aspects, *IP Multimedia Subsystem (IMS), Stage 2*, 3GPP TS 23.228 v 5.9.0 (2003-06), 127 pages, 2003.

[6] BOYLE, J. et al., *The COPS (Common Open Policy Service) Protocol*, rfc 2748, IETF, http://www.faqs.org/rfcs/rfc2748.html, 38 pages, jan. 2000.

[7] CHAN, K. et al., *COPS Usage for Policy Provisioning (COPS-PR)*, rfc 3084, IETF, http://www.faqs.org/rfcs/rfc3084.html, 34 pages, mars 2001.

[8] YAVATKAR, R. et al., *A Framework for Policy-Based Admission Control*, rfc 2753, http://www.faqs.org/rfcs/rfc2753.html, 20 pages, jan. 2000.

[9] 3GPP Technical Specification Group Services and System Aspects, *Policy control over Go interface*, 3GPP TS 29.207 v5.4.0 (2003-06), 55 pages, 2003.

[10] 3GPP Technical Specification Group Services and System Aspects, *End-to-End quality of service (QoS) signaling flows*, 3GPP TS 29.208 v5.4.0 (2003-06), 26 pages, juin 2003.

[11] ZHUANG, W. et al., «Policy-Based QoS Architecture in the IP multimedia Subsystem of UMTS», *IEEE Network*, vol. 17, no 3, IEEE, pp. 52-57, mai/juin 2003.

[12] KRISHNAMOORTHY, P., *Chapter 2 Self-similarity and long range dependance*, http://www.utdallas.edu/~sanna/chapter2.pdf, pp. 1-12, nov. 2002.

[13] HYYTIÄ, E., *Characterization of Internet Traffic*, http://keskus.hut.fi/opetus/s38149/s99/reports/1011esa.pdf, pp. 1-14, oct. 1999.

[14] HAMITI, S., *Heavy-Tailed Distributions in traffic modeling*, http://keskus.hut.fi/opetus/s38149/s99/reports/1115shkumbin.doc, pp. 1-13, nov. 1999.

[15] CROVELLA, M. E. et BESTAVROS, A. «Self-Similarity in World Wide Web: Evidence and Possible Causes», New York, *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, IEEE, pp. 835-846, déc. 1997.

[16] JIANG, H. et DOVROLIS, C., «Source-Level IP Packet Bursts: Causes and Effects», *in Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement (IMC'03)*, Miami Beach, ACM, pp. 301-306, oct. 2003.

[17] GUO, L. et al., «How Does TCP Generate Pseudo-Self-Similarity?», *in Proceedings of the Ninth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems*, Cincinnati, IEEE, pp. 215-223, août 2001.

[18] VERES, A. et BODA, M., «The Chaotic Nature of TCP Congestion Control», Tel Aviv, *in Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM 2000)*, vol. 3, no 26-30, IEEE, pp. 1715 - 1723, mars 2000.

[19] GARRETT, M., et WILLINGER, W., «Analysis, Modeling and Generation of Self-Similar VBR Video Traffic», *in Proceedings of the conference on Communications architectures, protocols and applications*, vol. 24, no 4,

London, ACM SIGCOMM Computer Communication Review, pp. 269-280, sept. 1994.

[20] BERAN, J. et al. «Long-Range Dependance in Variable-Bit-Rate Video Traffic», *IEEE Transactions on Communications*, vol. 43, no. 2-4, IEEE, pp. 1566-1579, sept. 1995.

[21] KRUNZ, M. et TRIPATHI, S. K., «On the Characterization of VBR MPEG Streams», *in Proceedings of the 1997 ACM SIGMETRICS international conference on Measurement and Modeling of Computer Systems*, Seattle, ACM SIGMETRICS Performance Evaluation Review, vol. 25, no 1, pp. 192-202, Seattle, juin 1997.

[22] DOWNEY, A. B., «Evidence for Long-Tailed distributions in the Internet», *in Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, San Francisco, ACM, pp. 229-241, nov. 2001.

[23] FISCHER, M. J. et FOWLER, T. B. «Fractals, Heavy-Tails, and the Internet», Mitretek Technology Summaries, http://www.mitretek.org/pubs/mitretek-summaries_summer/Sigma_Pubs/Fractals.PDF, pp. 11-16, été 2001.

[24] BRESLAU, L. et al., «Comments on the Performance of Measurement-Based Admission Control Algorithms», Tel Aviv, *in Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM 2000)*, vol. 3, no. 1, pp. 1233-1242, mars 2000.

[25] DE MEER et al., *Analysis of Existing QoS Solutions*, internet draft, IETF, http://www.rnp.br/ietf/internet-drafts/draft-demeer-nsis-analysis-03.txt, 29 pages, nov. 2002.

[26] MINEI, I., *MPLS DiffServ-aware Traffic Engineering*, white paper, Juniper Networks, http://www.juniper.net/solutions/literature/white_papers/200048.pdf, 25 pages, 2004.

[27] SEMERIA, C., *Supporting Differentiated Service Classes: Multiprotocol Label Switching (MPLS)*, white paper, Juniper Networks,

http://www.juniper.net/solutions/literature/white_papers/200039.pdf, 18 pages, 2002.

[28] *MPLS protocols Family*, http://www.protocols.com.

[29] *Qbone Bandwidth Broker Architecture*, work in Progress, http://qbone.internet2.edu/bb/bboutline2.html, juin 2000.

[30] LI, M., *MPLS Traffic Engineering Policy Information Base*, internet draft, IETF, http://www.dfn-pca.de/bibliothek/standards/ietf/none/internet-drafts/draft-li-rap-mplspib-00.txt, 25 pages, fév. 2003.

[31] BOUCADAIR, M., *An IP Traffic Engineering PIB for Accounting purposes*, IETF, internet draft, http://ftp.scarlet.be/pub/documentation/internet-drafts/draft-boucadair-ipte-acct-pib-02.txt, 19 pages, juin 2003

[32] JACQUENET, C., *A COPS client-type for IP traffic engineering*, Work in Progress, IETF, http://www.watersprings.org/pub/id/draft-jacquenet-ip-te-cops-04.txt, 13 pages, déc. 2002.

[33] SRINIVASAN, C. et al., *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*, rfc 3812, IETF, http://www.ietf.org/rfc/rfc3812.txt , 68 pages, juin 2004

[34] AWDUCHE, D. et al., *Overview and Principles of Internet Traffic Engineering*, rfc 3272, IETF, http://rfc.sunsite.dk/rfc/rfc3272.html, 71 pages, mai 2002

[35] Avici Systems, Industry Background, http://www.avici.com/technology/industry_background.shtml, 2004

[36] Seeling. P. et al., «Network Performance Evaluation Using Frame Size and Quality Traces of Single-Layer and Two-Layer Video: A Tutorial», *IEEE Communications Surveys and Tutorials*, vol. 6, no. 2, IEEE, pp. 58-78, 2004

[37] Internet Traffic Archive, *Traces in the Internet Traffic Archive*, http://ita.ee.lbl.gov/html/traces.html, avr. 2000.

[38] NATARAJAN, V., *An algorithm for computing the inverse normal cumulative distribution function*, Computer implementations, http://home.online.no/~pjacklam/notes/invnorm/#C, sept. 2004

ANNEXES

A.1 Famille mondiale IMT-2000 et groupements 3GPP et 3GPP2

Tableau A.1 Famille IMT-2000

Technologie d'accès radio	***Nom officiel IMT-2000***	***Consortium support***
UTRA/FDD *Universal Terrestrial Radio Access Frequency Division Duplex*	IMT-DS *International Mobile Telecommunications Direct Spread*	3GPP et ETSI *European Telecommunications Standards Institute*
UTRA/TDD *Universal Terrestrial Radio Access Time Division Duplex*	IMT-TC *International Mobile Telecommunications Time Code*	
TD/SCDMA *Time Division Synchronous Code Division Multiple Access*		CWTS *China Wireless Telecommunication Standard Group*
CDMA-2000	IMT-MC *International Mobile Telecommunications Multi-carrier*	3GPP2
UWC-136 *Universal Wireless Communications*	IMT-SC *International Mobile Telecommunications Single carrier*	UWC *Universal Wireless Communications*
DECT *Digital Enhanced Cordless Telecommunications*	IMT-FT *International Mobile Telecommunications Frequency Time*	

Tableau A.2 Groupements 3GPP et 3GPP2 de UMTS et de cdma2000

Groupement	3GPP	3GPP2
Date de création	Janvier'99	Janvier'99
Technologie	UMTS	Cdma2000
Organismes affiliés	ETSI (Europe), TTA (Corée), TTC (Japon), ARIB (Japon), T1 (É.-U.), CWTS (Chine)	TTA (É.-U.), TTA (Corée), TTC (Japon), ARIB (Japon), CWTS (Chine)
Type de réseau cœur	GSM-GPRS	ANSI-41
Technologie du réseau d'accès	DS-W-CDMA (FDD) TD/CDMA (TDD)	DS/MC-W-CDMA (IS-95)

A.2 Évolution de UMTS à travers les releases

Tableau A.3 Évolution de UMTS à travers les releases

Vers le tout-ip ↑

Releases	*Contributions majeures*
R 6	**- Phase 2 du sous-système *IMS IP Multimedia Subsystem*** - Harmonisation des IMS de 3GPP et 3GPP2, inter-fonctionnement UMTS–WLAN, etc.
R5	**- Développement du réseau cœur** - IMS : usage de protocoles de l'IETF (Ipv6, SIP, *Diameter*) - Qualité de service pour IMS (autorisation de QdS, contrôle basé sur des politiques et compression SIP) - GERAN – UMTS et améliorations diverses, ex. W-CDMA
R 4	**- Release d'importance moindre** - Améliorations à l'UTRAN, évolution du domaine CS, transport IP pour les protocoles du réseau cœur, et autres améliorations
R 99	**- Développement du réseau d'accès** - Nouvelle interface radio – W-CDMA - Nouvelle architecture pour le réseau d'accès radio UTRAN et relève « soft » **- Inter-fonctionnement GSM-UMTS**

A.3 Attributs de QdS du service de support UMTS

Tableau A.4 Valeurs possibles pour les attributs de QdS du service support UMTS

	Conversational	Streaming	Interactive	Background
Maximum bitrate (kbps)	<= 2 048 (1) (2)	<= 2 048 (1) (2)	<= 2 048 - overhead (2) (3)	<= 2 048 - overhead (2) (3)
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)	<=1 500 or 1 502 (4)
SDU format information	(5)	(5)		
Delivery of erroneous SDUs	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)
SDU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100 – maximum value	280 (8) – maximum value		
Guaranteed bit rate (kbps)	<= 2 048 (1) (2)	<= 2 048 (1) (2)		
Traffic handling priority			1,2,3	
Allocation/ Retention priority	1,2,3	1,2,3	1,2,3	1,2,3
Source statistic descriptor	Speech/unknown	Speech/unknown		
Signalling Indication			Yes/No	

A.4 Fonctions de gestion de QdS sur le plan de transmission UMTS

Les fonctions de gestion de QdS UMTS sur le plan de transmission assurent le respect du contrat de QdS qui est établi pour le service de support UMTS. Elles bornent les trafics de signalisation et de données usager. Elles regroupent la fonction de mise en correspondance, la fonction de classification, le gestionnaire de ressources et le module de conditionnement de trafic. Elles sont illustrées à la Figure A.1.

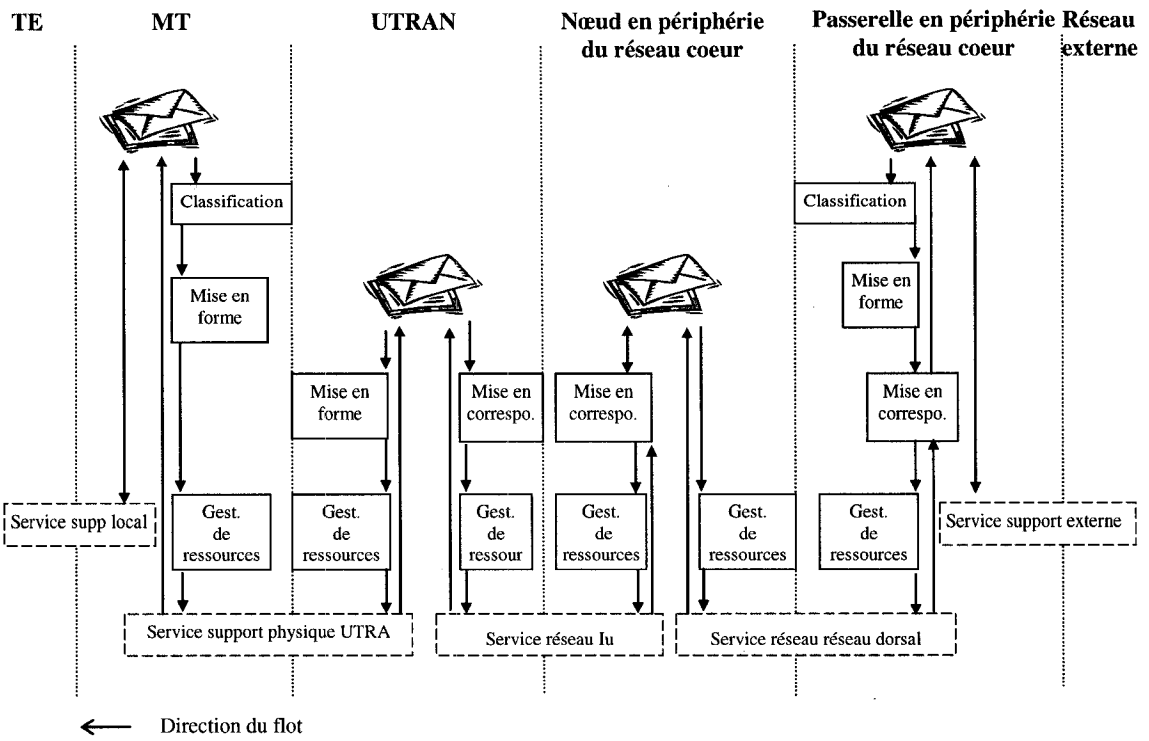

Figure A.1 Fonctions de gestion de QdS sur le plan de transmission UMTS

A.5 Sous-système multimédia IMS

A.5.1 Composantes IMS (sans le HSS et les CSCF)

Le sous-système multimédia IMS abrite le serveur local des abonnés HSS (*Home Subscriber Server*), les serveurs SIP CSCF (*Call State/Service Control Function*) ainsi que les entités d'inter-fonctionnement dédiées au contrôle et à la conversion des données. Les nœuds sont ici expliqués, à l'exception des CSCF et du HSS. La Figure A.2 illustre l'architecture du sous-système IMS.

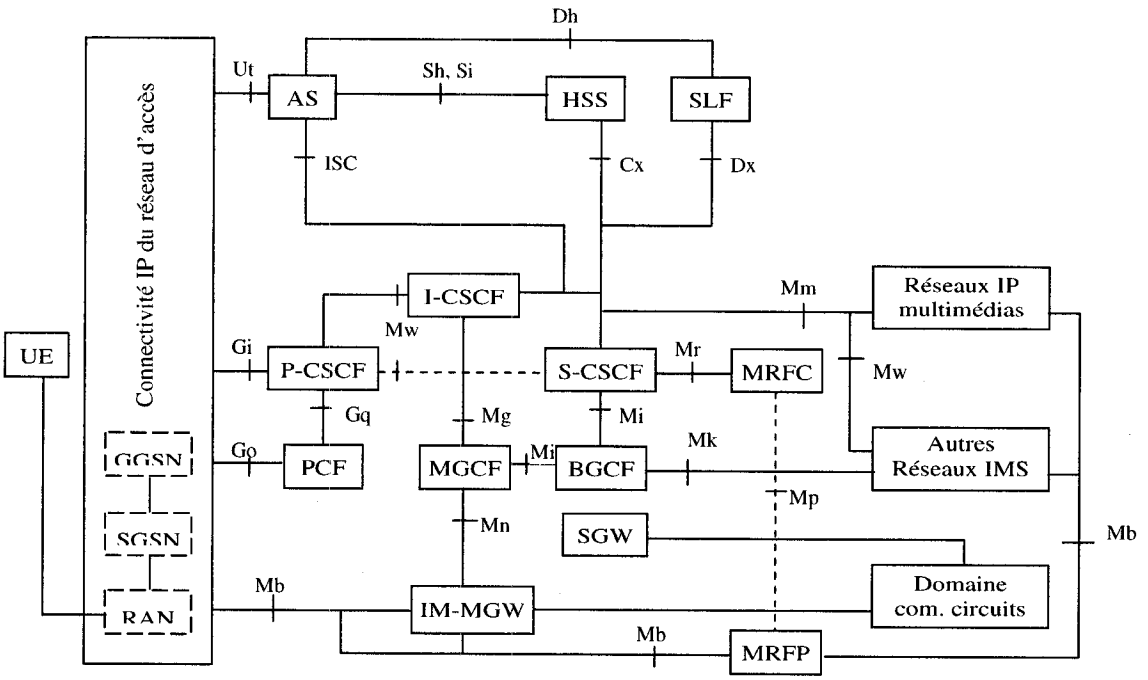

Figure A.2 Architecture du sous-système multimédia IMS

En plus des nœuds CSCF, le sous-système héberge la fonction de contrôle de la passerelle media (*Media Gateway Control Function MGCF*). Celle-ci gère un ou plusieurs nœuds MGW via l'interface Megaco et comprend la fonction IM-SSF. Elle effectue aussi la conversion des messages de signalisation entre le format SIP et celui du réseau *legacy*, notamment entre SIP et ISUP (ISDN User Part du sous-système

utilisateur du réseau *legacy*) afin de communiquer, via la fonction T-SGW, avec l'interface de signalisation du RTC. Elle transforme aussi en messages Megaco les messages de signalisation SIP destinés à la fonction *MGW* (qui peut lui être intégrée).

De plus, on trouve la fonction passerelle media qui porte l'acronyme anglais *MGW* (*Media Gateway Function*). Elle réalise la commutation, le transcodage et la transmission média. Elle effectue aussi la conversion des données qui doivent être acheminées entre des nœuds de réseaux différents (surtout entre le RTC et IP).

En outre, le sous-système inclut la fonction des ressources multimédias *MRF Multimedia Resource Function.* Celle-ci permet de supporter une variété de fonctionnalités propres à IMS, notamment, les services de conférence média et l'établissement simultané d'appels multimédias entre plusieurs intervenants. Elle se compose du *MRFC Multimedia Resource Function Controller* et du *MRFP Multimedia Resource Function Processor.*

Quant à la fonction passerelle de signalisation de transport, elle est dénommée *T-SGW* pour *Transport Signaling Gateway Function.* Elle convertit les messages de signalisation ISUP basés sur IP du *MGCF* en messages basés sur SS7 du RTC. Donc, le *MGCF* ne supporte pas SS7. Pour finir, le sous-système IMS contient la fonction passerelle de contrôle de transition (*BGCF Breakout Gateway Control Function*). Celle-ci choisit le *MGCF* et le *MGW* pour la transition avec un réseau *legacy*.

A.5.2 Procédures IMS

Les procédures peuvent être liées à la session ou non. Elles incluent, entre autres choses, l'établissement d'un contexte PDP pour la signalisation IMS, la découverte d'un CSCF local ainsi que l'affectation, l'annulation et la ré-affectation d'un S-CSCF à un usager. D'autres procédures sont aussi définies.

Établissement d'un contexte PDP pour la signalisation IMS

Le trafic de contrôle associé aux applications IMS est convoyé dans un contexte PDP établi au préalable. Le contexte activé peut être dédié à la signalisation IMS ou

général dans le cas où l'usager ne solliciterait pas le premier type de contexte ou dans le cas où l'opérateur ne le supporterait pas (*general purpose PDP context* et *dedicated signaling PDP context*). Le contexte dédié est sujet à des règles et restrictions définies par l'opérateur. Pour le moment, elles sont renforcées au niveau du GGSN et elles indiquent les destinations possibles pour ce dernier, soient le P-CSCF et les serveurs DHCP et DNS locaux. De plus, l'usager peut préciser le niveau de contexte PDP :

- lors de la procédure d'activation de contexte, l'usager peut inclure le drapeau de signalisation IMS (*IM CN Subsystem Signaling Flag*) dans le PCO IE et l'indication de signalisation (*Signaling Indication*) dans l'élément QoS IE (*QoS Information Element*). Ceci indique aux sous-réseaux cœur et radio que le contexte PDP, une fois négocié avec le réseau, doit être privilégié au niveau du réseau radio (avec les règles et restrictions);

- lors de la procédure d'activation de contexte, il peut inclure strictement le drapeau de signalisation IMS dans le PCO IE afin de spécifier au réseau GPRS que le contexte PDP sollicité devra être utilisé pour la signalisation des applications (règles et restrictions);

- l'usager peut aussi solliciter un contexte PDP général avec un profil négocié de QdS.

Découverte d'un CSCF local

Deux alternatives sont possibles pour la découverte du P-CSCF.

a) Découverte d'un CSCF local basée sur DHCP/DNS

Après l'activation d'un contexte PDP pour la signalisation IMS, l'usager interagit avec la passerelle GGSN afin d'obtenir le nom d'un P-CSCF et les adresses IP des serveurs DNS afin d'obtenir du DNS une liste de P-CSCFs. Il en sélectionne un par la suite. La Figure A.3 montre cette procédure.

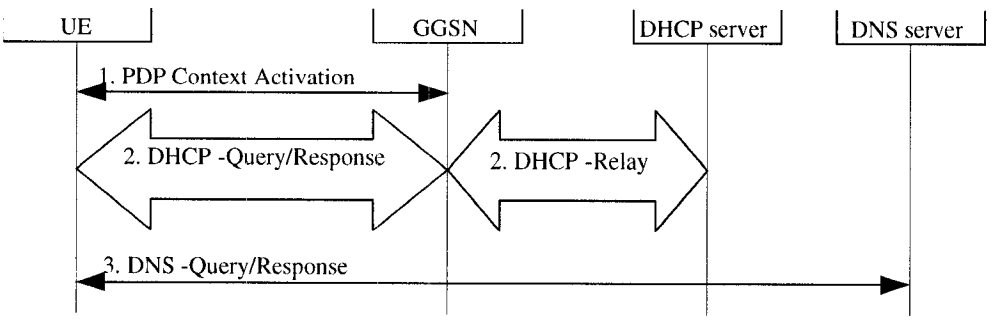

Figure A.3 Découverte du P-CSCF basée sur DNS/DHCP

b) Découverte d'un CSCF local basée sur une procédure GPRS

L'adresse du P-CSCF est obtenue du GGSN lors de la procédure d'activation de contexte par un mécanisme propre à l'opérateur. Si l'usager ne supporte pas DHCP, cette procédure est employée. La Figure A.4 illustre les étapes de cette méthode.

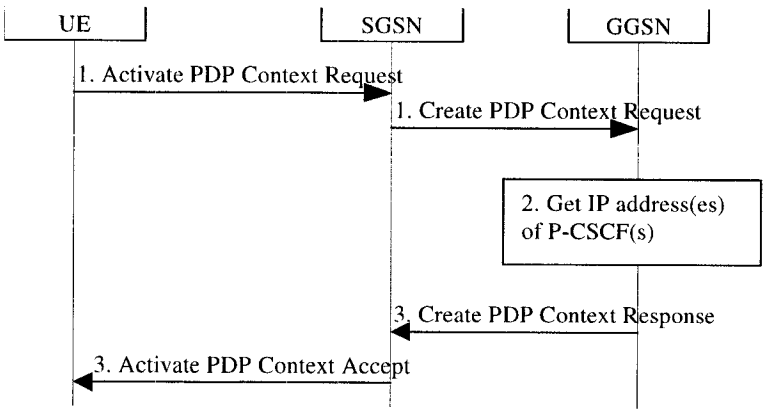

Figure A.4 Découverte d'un CSCF local basée sur une procédure GPRS

Procédures liées à l'affectation d'un S-CSCF à un usager

Ces procédures comprennent l'affectation, l'annulation et la ré-affectation d'un S-CSCF à un usager. Elles sont exécutées par le nœud I-CSCF dans le but de répondre aux requêtes d'enregistrement des usagers.

Autres procédures

En ce qui a trait aux procédures liées au I-CSCF, plusieurs I-CSCFs peuvent se trouver dans le réseau d'un même opérateur. La sélection de l'I-CSCF peut se fonder sur des mécanismes DNS et dépendre, par exemple, de la localisation et de l'identité du nœud. En ce qui concerne le P-CSCF, le routage de l'information SIP relative à l'enregistrement ne doit considérer les enregistrements antérieurs, mais le routage des messages de la session doit considérer l'information obtenue au cours de la procédure d'enregistrement. Le même chemin doit être emprunté. Des procédures pour la mise à jour de l'information usager du S-CSCF sont effectuées si l'information de souscription du HSS est modifiée (le serveur d'abonnés envoie alors les changements au S-CSCF). Les procédures d'enregistrement, d'annulation d'enregistrement sont aussi réalisées. Quant à la gestion basée sur les politiques sur les services, elle s'appuie sur des procédures qui seront explicitées ultérieurement. Noter que d'autres procédures n'ayant aucun rapport avec la session proprement dite sont prévues.

A.6 Objets et messages COPS

Les messages COPS possèdent un en-tête et plusieurs objets, ceux-ci comportent aussi leur propre en-tête.

A.6.1 Description des messages COPS

Il existe dix messages COPS pour la communication entre le serveur et le client de politiques. Ils sont décrits dans les lignes qui suivent.

- *Request (REQ)*

Ce message est généré par le PEP pour envoyer un *request client state handle* au PDP. Celui-ci l'utilise pour envoyer au PEP des décisions sur la connexion TCP pour un type de client donné. Les modifications à cette requête peuvent être effectuées avec

une requête donnant le « handle » fourni. Le PEP envoie aussi des requêtes pour informer le PDP des changements internes (mises à jour).

- *Decision (DEC)*

Le PDP répond au PEP en lui envoyant une décision précisant l'objet handle de la requête du client et d'autres informations. Un code d'erreur est retourné en cas d'erreur.

- *Report State (RPT)*

Ce message est utilisé par le PEP pour informer le PDP du résultat de l'exécution d'une de ses décisions (succès/échec) ou pour lui rapporter un changement d'état à caractère comptable. Ce message peut être transmis sur une base périodique pour fournir des informations pour les fins de gestion et de contrôle. Il spécifie l'objet handle.

- *Delete Request State (DRQ)*

Ce message est utilisé par le PEP pour notifier le PDP de la désuétude d'un handle. Il conduit à la suppression dans le PDP de l'état de la requête. La raison du retrait est indiquée et doit être interprétée en fonction du type de client COPS. Si ce message n'est pas envoyé au PDP, l'état associé à la requête est conservé jusqu'à la fermeture de la connexion ou jusqu'à la terminaison de la session client. Les décisions mal formulées doivent déclencher une requête DRQ qui précise le code d'erreur. L'état associé doit être effacé ou re-sollicité.

- *Synchronize State Req (SSQ)*

Ce message permet au PDP de demander au client un état. Si une valeur est donnée pour l'objet handle, seul l'état associé doit être synchronisé. S'il n'est pas reconnu par le PEP, ce dernier doit transmettre une requête DRQ au PDP. Si le message

SSQ ne fournit pas de valeur pour l'objet handle, tous les états actifs doivent être synchronisés avec le PDP. Le PEP fait la synchronisation en renvoyant des requêtes pour l'état existant dans le PEP et pour le type de client spécifié. Au terme de cette étape, le PEP achemine un message *Synchronize Complete*.

- *Client-Open (OPN)*

Dans ce message, le PEP spécifie les types de clients qu'il peut supporter, le dernier PDP auquel il était connecté pour le type de client et/ou des caractéristiques de négociation spécifiques au client. Si le PDP reçoit un message OPN incohérent, il doit générer un message *Client-Close*.

- *Client-Accept (CAT)*

Ce message est envoyé par le PDP pour répondre favorablement à une requête OPN. Il inclut un objet *timer* (minuterie) qui définit l'intervalle entre deux keep-alive (en secondes). Une minuterie indiquant le temps minimum peut aussi être spécifiée ainsi qu'une autre donnant l'intervalle maximum entre deux messages périodiques de rapports de contrôle pour une valeur donnée de l'objet handle. Si le PEP reçoit un message CAT incohérent, il doit générer un message Client-Close.

- *Client-Close (CC)*

Ce message conduit à la fermeture de la connexion. Il peut être généré par le PEP (PDP) pour informer le PDP (PEP) qu'un type de client n'est plus supporté. Le PDP peut fournir au PEP l'adresse d'un PDP alternatif qui supporte le type de client mentionné dans l'en-tête.

- *Keep-Alive (KA)*

Ce message permet de suivre l'état d'une connexion. Il est transmis à des intervalles au plus égaux à la valeur minimale des intervalles donnés par les minuteries

KA des messages CAT (entre les valeurs ¼ et ¾ de cet intervalle). Sur réception d'un message KA, le PDP fait écho en renvoyant un message KA au PEP. La valeur nulle est inscrite dans le champ *Client-Type* de l'en-tête. Si la connexion est défectueuse, le PEP doit essayer de se connecter à un serveur de politiques alternatif

- *Synchronize Complete (SSC)*

Ce message est envoyé par le PEP au PDP sur réception d'une requête de synchronisation SSQ de celui-ci. La synchronisation souhaitée doit avoir été effectuée. L'objet handle ne doit être précisé que si le message SSQ référençait une valeur spécifique de l'objet handle.

A.6.2 Format de l'en-tête commun des messages COPS

L'en-tête des messages COPS a un format bien spécifique. Il est montré à la Figure A.5.

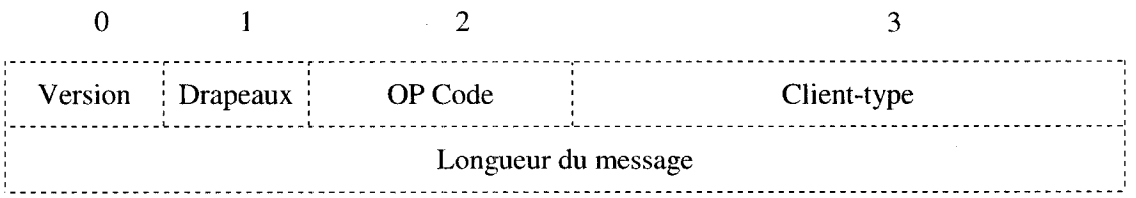

Figure A.5 En-tête des messages COPS

Les cinq champs de l'en-tête sont décrits dans le Tableau A.5 sur la page suivante.

Tableau A.5 Description des champs de l'en-tête commun des messages COPS

Champ	*Nombre de bits*	*Description*
Version	4	Numéro de version COPS (version courant est 1)
Drapeaux	4	Valeurs de drapeaux définies (les autres doivent être mises à zéro). 0x1 : Bit pour le drapeau d'un message sollicité, marqué si ce message est demandé par un autre. Autrement, sa valeur est nulle.
OP Code	8	- Indique l'opération COPS : 1 = Request (Req) 6 = Client-Open (OPN) 2 = Decision (Dec) 7 = Client-Accept (CAT) 3 = Report State (Rpt) 8 = Client-Close (CC) 4 = Delete Request State (DRQ) 9 = Keep-Alive (KA) 5 = Synchronize State Req (SSQ) 10 =Synchronize Complete (SSC)
Client-type	16	- Indique le type de client et le cadre d'interprétation des objets - Si bit le plus significatif marqué: enteprise-specific 0x8000–0xFFFF - Pour les messages KA, client-type = 0
Longueur du message	32	- Longueur du message en octets, incluant l'en-tête COPS et les objets encapsulés. Les messages doivent être alignés sur des intervalles de quatre octets.

A.6.3 Format des objets des messages COPS

Les objets COPS comportent un en-tête de quatre octets. La Figure A.6 illustre l'en-tête et le Tableau A.6 décrit les objets contenus dans l'en-tête.

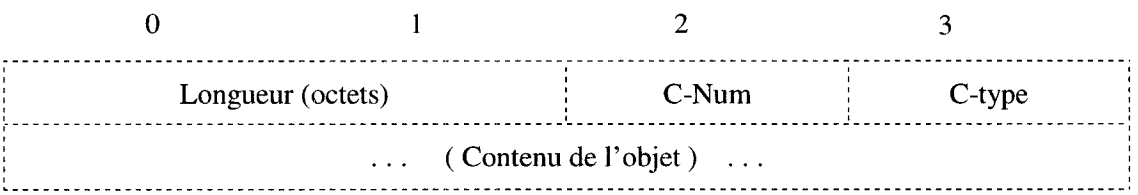

Figure A.6 Format d'un objet inclus dans un message COPS

Tableau A.6 Description des champs de l'en-tête des objets des messages COPS

Champ	*Nombre de bits*	*Description*
Longueur	16	- Longueur de l'objet, incluant l'en-tête. Les messages doivent être alignés sur des intervalles de quatre octets (« padding » si nécessaire).
C-Num	8	- Identifie la classe de l'information renfermée dans l'objet : 1 = Handle 2 = Context 3 = In Interface 4 = Out Interface 5 = Reason Code 6 = Decision 7 = LPDP Decision 8 = Error 9 = Client Specific Info 10 = Keep-Alive Timer 11 = PEP Identification 12 = Report type 13 = PDP Redirect Address 14 = Last PDP Address 15 = Accounting timer 16 = Message Integrity
C-type	8	- Valeurs définies par C-Num.

Les valeurs de C-Num et de C-Type caractérisent donc l'objet. Les classes d'information sont présentées ici.

- Objet *Handle* (*Handle*) *C-Num = 1 C-Type = 1*

Cet objet identifie de manière unique un état installé pour une requête PEP. Ce champ est de longueur variable et est unique pour un client PEP et une connexion donnés. Il est toujours choisi initialement par le PEP et supprimé par celui-ci lorsque désuet. Il doit être installé au niveau du PDP et spécifié dans les messages REQ, RPT et Delete envoyés au PDP

- Objet *Context* (*Context*) *C-Num = 2 C-Type = 1*

Cet objet indique le type de l'événement qui a déclenché la génération et l'envoi de cette requête. Il est requis pour les messages de REQ. Noter que les requêtes de contrôle d'admission, d'allocation des ressources, de configuration et d'acheminement peuvent donner lieu à un approvisionnement extérieur de politiques auprès d'un serveur

PDP. Pour certains types de clients, le PEP peut soumettre une requête pour recevoir une information de configuration du PDP, laquelle information peut prendre la forme de paramètres de configuration du PEP ou encore de règles de politiques vérifiables par le PEP. Plusieurs drapeaux peuvent être marqués pour une même requête. La Figure A.7 illustre le format de cet objet.

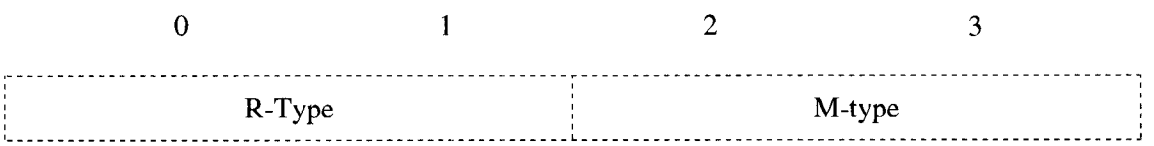

Figure A.7 Format de l'objet *Context*

R-Type (drapeau du type de requête)

0x01 = Message entrant / Requête de contrôle d'admission
0x02 = Requête d'allocation de ressources
0x04 = Requête de message sortant
0x01 = Requête de configuration

M-Type (type du message)

Valeurs sur seize bits spécifiques au client indiquant les types de messages du protocole

- Objet *In-Interface* (*In-Int*)

Cet objet révèle l'interface d'entrée de la requête et l'adresse de provenance du message. Pour les messages générés par l'hôte local, l'adresse *loopback* et le champ *ifindex* sont utilisés. L'interface entrante est spécifiée à l'aide du dernier champ. Il peut différencier des sous-interfaces. Les valeurs pour C-Num et C-Type sont les suivantes :

C-Num = 3 C-Type = 1 IPv4 address + interface
C-Num = 3 C-Type = 2 IPv6 address + interface

Le format de l'en-tête est montré à la Figure A.8 pour une adresse IPv4. Pour une adresse IPv6, l'espace réservé est plus grand.

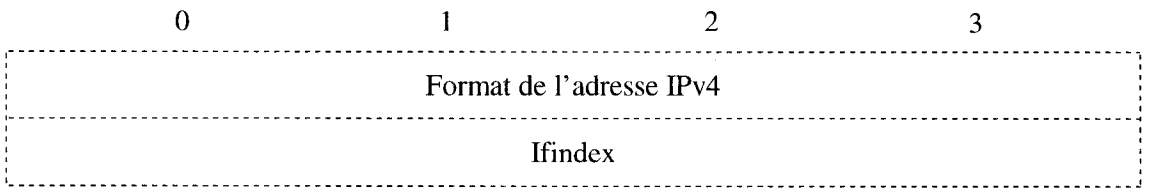

Figure A.8 Format des objets *In-Int* et *Out-Int*

- Objet *Out-Interface* (*Out-Int*)

Cet objet révèle l'interface de sortie à laquelle s'applique la requête ainsi que l'adresse de destination du message. Pour les messages destinés vers l'hôte local, l'adresse *loopback* et le champ *ifindex* sont utilisés. L'interface de sortie est spécifiée à l'aide du dernier champ. Il peut différencier des sous-interfaces. Les valeurs pour C-Num et C-Type sont les suivantes :

- C-Num = 4 C-Type = 1 IPv4 address + interface
- C-Num = 4 C-Type = 2 IPv6 address + interface

Les formats sont les mêmes que ceux pour l'objet *In-Int* (Figure A.8).

- Objet *Reason* (*Reason*)

Cet objet donne la raison de suppression de l'état d'une requête et apparaît dans un message DRQ. Le format est montré à la Figure A.9. Le champ *Reason Sub-Code* donne un code spécifique au client.

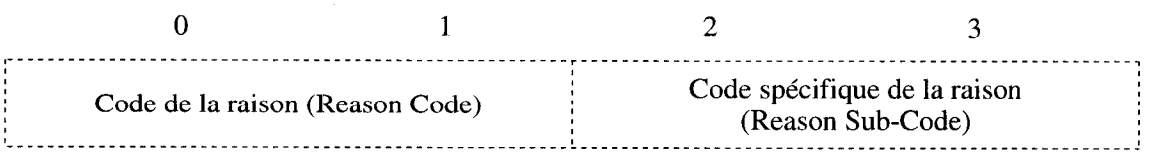

Figure A.9 Format de l'objet *Reason*

Code de la raison

1 = Non spécifié
2 = Gestion
3 = Préemption par une autre requête
4 = Fermeture (pour communiquer une suppression signalée)
5 = Expiration de la minuterie de l'état local
6 = Changement de route invalidant l'état associé à la requête
7 = Manque de ressources locales
8 = Directive du PDP (décision de suppression par le PDP)
9 = Décision du PDP non supportée
10 = « Synchronize handle » inconnu
11 = « Handle » transitoire (événement sans état)
12 = Décision mal formulée
13 = Objet COPS envoyé par le PDP inconnu ; le Reason Sub-code donne les valeurs C-Num et C-Type associées à cet objet inconnu

➢ Objet *Decision* (*Decision*)

Cet objet est généré par le PDP et inséré dans des réponses. Les champs obligatoires pour cet objet dépendent entièrement du type du client.

- C-Num = 6 C-type = 1, drapeaux de décision (*decision flags*) ⇐ obligatoire

La Figure A.10 illustre cet objet.

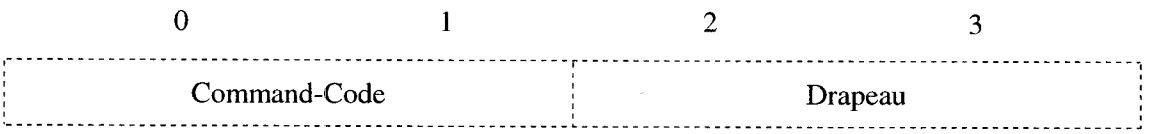

Figure A.10 Format de l'objet *Decision*

Commands

0 = Null Decision (donnée de configuration non disponible)
1 = Install (Admettre la requête / Installer l'information de configuration)
2 = Remove (Refuser la requête / Supprimer l'information de configuration)

Flags (drapeaux)

0x01 = Erreur détectée

- C-Num = 6 C-type = 2, donnée sans état (*stateless data*)

Ce type d'objet fournit de l'information sans état additionnelle pouvant être appliquée par le PEP localement. Il est de longueur variable ; son format doit être précisé dans un document décrivant l'extension COPS pour le type de client. Il est optionnel et doit être interprété en fonction de la valeur de l'objet *Context*. Par ailleurs, même les clients PEP censés faire un approvisionnement extérieur de politiques sont en mesure de prendre des décisions sans état simples grâce à leur serveur local LPDP.

- C-Num = 6 C-type = 3, donnée de substitution (*replacement data*)

Cet objet fournit les données devant remplacer celles indiquées dans un message signalé. Il est de longueur variable ; son format est précisé dans le document d'extension du client COPS. Il est optionnel et doit être interprété en fonction de l'objet *Context*.

- C-Num = 6 C-type = 4, donnée spécifique au client (*client-specific dec. data*)

Cet objet permet de préciser des types de décision additionnels. Il est de longueur variable ; son format est précisé dans le document d'extension du client COPS. Il est optionnel et doit être interprété en fonction de la valeur de l'objet *Context*.

- C-Num = 6 C-type = 5, donnée nommée de décision (*named decision data*)

L'information de configuration nommée doit être placée à l'intérieur de cette version de l'objet de décision (en réponse à des requêtes de configuration). Il est de longueur variable ; son format est précisé dans le document d'extension du client COPS. Il est optionnel et doit être interprété en fonction de la valeur de l'objet *Context* et des drapeaux de décision.

➢ Objet *LPDP Decision* (*LPDP Decision*)

Cet objet correspond à la décision du serveur LPDP local. Il peut être inséré dans les requêtes. Son format est semblable à celui des objets de décision spécifiques au client. Les valeurs C-Num et C-Type sont :

C-Num = 7 C-Type = valeurs de l'objet *Decision*

➢ Objet *Error* (*Error*) C-Num = 8 C-Type = 1

Cet objet identifie une erreur de protocole COPS. Le format est montré à la Figure A.11. Le champ *Error Sub-Code* donne un code spécifique au client.

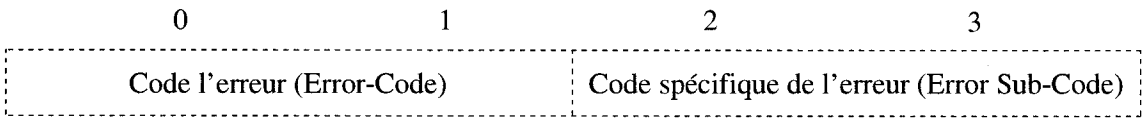

Figure A.11 Format de l'objet *Error*

Les codes d'erreurs possibles sont nombreux.

Error Code

1 = Mauvais « handle »
2 = Référence « handle » non valide
3 = Format de message incorrect
4 = Échec de traitement par le serveur
5 = Information obligatoire spécifique au client manquante
6 = Type de client non supporté
7 = Objet COPS obligatoire manquant
8 = Panne du client
9 = Problème de communication (panne)
10 = Non spécifié
11 = « Shutting down »
12 = Re-direction vers un serveur préférable
13 = Objet COPS inconnu ; le *Reason Sub-code* donne les valeurs C-Num et C-Type de celui-ci
14 = Échec d'authentification
15=Authentification requise

➢ Objet *Client-Specific Information* (*ClientSI*)

Cet objet de longueur variable peut être inséré dans les messages de requêtes, d'ouverture et de rapport d'exécution des décisions. Il contient une information spécifique au client et peut être de deux types.

- C-Num = 9 C-type = 1, information signalée spécifique au client (*Signaled ClientSi*)

Les objets/attributs spécifiques à un protocole de signalisation du client ou à son état interne sont placés à l'intérieur d'un ou de plusieurs objets *Signaled ClientSi*. Leur format est déterminé par le type du client.

- C-Num = 9 C-type = 2, information nommée spécifique au client (*Named ClientSI*)

Lorsqu'il est de ce type, l'objet *ClientSI* contient de l'information de configuration nommée utile pour relayer au serveur PDP une information se rapportant à un PEP, une requête ou encore à un état configuré.

➢ Objet *Keep-Alive Timer* (*KATimer*)

Le temps est spécifié sur deux octets en secondes (valeur delta). Cet objet indique l'intervalle de temps maximum pour l'émission ou la réception d'un message. Le domaine de valeurs est [1-65535] et une valeur nulle indique l'infini. Son format est donné à la Figure A.12.

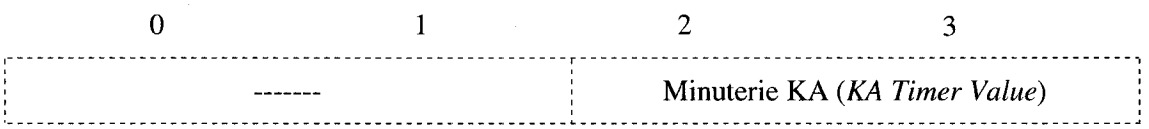

Figure A.12 Format de l'objet *KATimer*

➢ Objet *PEP Identification* (*PEPID*) C-Num = 11 C-Type = 1

Cet objet de longueur variable donne l'identifiant du PEP au PDP. Il est inclus dans les messages *Client-Open*. Il peut être utilisé par le PDP pour identifier le PEP dans les règles de politiques.

➢ Objet Report-Type (Report-Type) C-Num = 12 C-Type = 1

Cet objet indique le type du rapport associé à l'état de la requête avec un objet handle. Son format est montré à la Figure A.13.

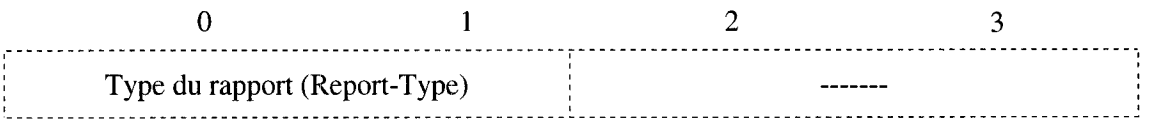

Figure A.13 Format de l'objet *Report-Type*

Report-Type

0 = *Success* : réussite de l'exécution de la décision au niveau du PEP
1 = *Failure* : échec de l'exécution de la décision au niveau du PEP
2 = *Accounting* : mise à jour liée à la comptabilité pour un état installé

➢ Objet *PDP Redirect Address* (*PDPRedirAddr*)

Cet objet est employé par le PDP pour fournir au PEP lors de la fermeture d'une connexion l'adresse d'un serveur PDP et un numéro de port TCP pour un type de client donné. Il est facultatif. Le format est illustré à la Figure A.14 lorsqu'une adresse IPv4 est utilisée (l'espace pour une adresse IPv6 est plus grand).

- C-Num = 13 C-type = 1, IPv4 Address + numéro de port TCP

- C-Num = 13 C-type = 2, IPv6 Address + numéro de port TCP

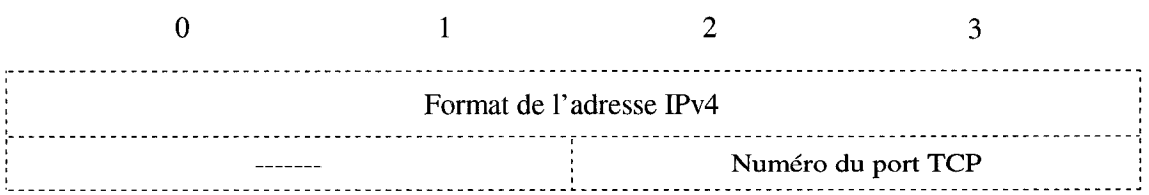

Figure A.14 Format de l'objet *PDP Redirect Address*

➢ Objet *Last PDP Address* (*LastPDPAddr*)

Le PEP insère dans le message *Client-Open* l'adresse du dernier PDP avec lequel il avait établi une connexion depuis la dernière initialisation. Cet objet n'est pas précisé si une connexion n'avait pas été établie. Il peut prendre deux valeurs *C-Type*:

- C-Num = 14 C-type = 1, *IPv4 Address* (même format que *PDPRedirAddr*)

- C-Num = 14 C-type = 2, *IPv6 Address* (même format que *PDPRedirAddr*)

➢ Objet *Accounting Timer* (*AcctTimer*) C-Num = 15 C-Type = 1

Le temps est spécifié sur deux octets en secondes (valeur delta). Cet objet indique l'intervalle de temps minimum entre deux messages de rapports de comptabilité périodiques successifs. Le domaine de valeurs est [1-65535]. Une valeur nulle signifie prohibe l'utilisation des rapports. Le format est montré à la Figure A.15.

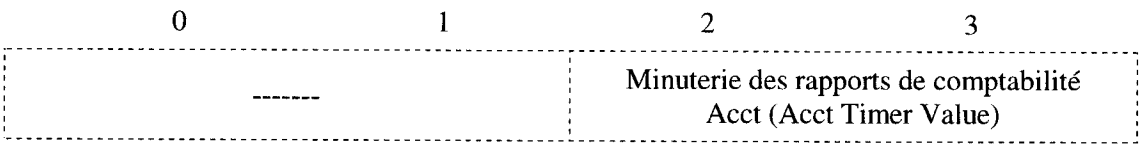

Figure A.15 Format de l'objet *Accounting Timer*

➢ Objet *Message Integrity* (*Integrity*) C-Num = 16 C-Type = 1 *HMAC digest*

Cet objet donne un numéro de séquence et un *HMAC digest* du message pour l'authentification et pour valider l'intégrité du message COPS. Il est placé à la fin du message COPS. Le format est présenté à Figure A.16.

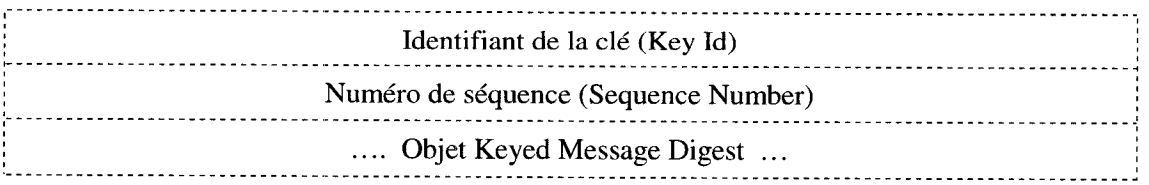

Figure A.16 Format de l'objet *Message Integrity*

A.7 Objets COPS-PR

A.7.1 Format des objets COPS-PR

Le modèle COPS-PR inscrit de nouveaux objets dans les objets *Named ClientSI* et *Named Decision Data*. La Figure A.17 donne les formats de ces objets. Les champs S-Num et S-Type sont semblables aux champs C-Num et C-Type mentionnés précédemment et sont associées aux clients COPS-PR.

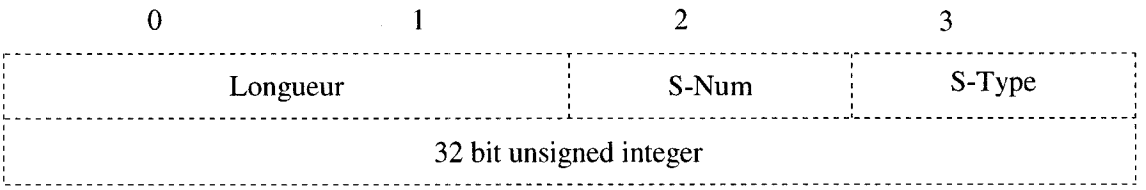

Figure A.17 Format des objets COPS-PR

A.7.2 Description des objets définis pour le modèle COPS-PR

Tableau A.7 Objets nouveaux de *Named ClientSi* et *Named Decision Data*

Objet COPS-PR	*Description*
Complete Provisioning Instance Identifier (PRID)	S-Num = 1 S-Type = 1 (BER) Length = variable - identifiant de l'instance
Prefix PRID (PPRID)	S-Num = 2 S-Type = 1 (BER) Length = variable - ne peut être utilisé que dans l'opération « Remove Decision » (pour des fins d'optimisation)
Encoded Provisioning Instance Data (EPD)	S-Num = 3 S-Type = 1 (BER) Length = variable - valeur encodée de l'instance
Global Provisioning Error Object (GPERR)	S-Num = 4 S-Type = 1 (BER) Length = 8 - format semblable à celui de l'objet Error de COPS - pour communiquer des erreurs générales non rattachées à une classe PRC particulière (code d'erreur + sous-code d'erreur) - par ex., *malformedDecision (11)*, *unknownCOPSPRObject (10)*, *unknownPIBData (9)* et *avaliableMemLow (1)* sont des codes définis
PRC Class Provisioning Error Object (CPERR)	S-Num = 5 S-Type = 1 (BER) Length = 8 - format semblable à celui de l'objet Error de COPS - pour communiquer des erreurs rattachées à une classe PRC particulière ; un objet ERROR PRID doit leur être associé - par ex., *priSpaceExhausted (1)*, *priInstanceInvalid (2)*, *unknownPrc (9)* et *tooFewAtrr (10)* sont des codes génériques spécifiques à des classes
Error PRID Object (ErrorPRID)	S-Num = 6 S-Type = 1 (BER) Length = variable - identificateur ou PRID de l'instance ayant causé une erreur d'installation ou qui n'a pas pu être installée ou supprimée

A.7.3 Format des objets COPS-PR convoyant de l'information spécifique au client

Le format *Client-Specific* est défini pour les objets inclus dans les objets *Named Decision Data* du message de décision, *Named ClientSI* d'une requête et, enfin, *Named ClientSI* du message Report. Ces objets sont expliqués dans les lignes qui suivent.

- *Named Decision Data*

Cet objet renferme généralement une ou plusieurs associations PRID-EPD (*bindings*). Dans une opération « remove », l'objet EPD ne doit pas être précisé, contrairement à dans une opération « install ». Le PRID ou le préfixe PRID doit toujours être indiqué. Comme on peut le voir ci-après, le contenu de l'objet *Named Decision Data* dépend du type de décision (*install/remove*).

<Named Decision Data> :: = <<Install Decision> | <Remove Decision>>
<Install Decision> :: = *(<PRID> <EPD>)
<Remove Decision> :: = *(<PRID>|<PPRID>)

- *ClientSI Request Data*

Le format de cet objet est :

<Named ClientSI: Request> ::= <*(<PRID> <EPD>)>

- *Policy Provisioning Report data*

L'objet *Named ClientSI* est employé avec l'objet COPS Report Type pour encapsuler l'information devant être envoyée par le PEP au PDP. Les types de rapports sont *Success*, *Failure* et *Accounting*. Les deux premiers indiquent au PDP le succès ou l'échec d'installation/suppression de politiques au niveau du PEP. Les associations ainsi que les codes d'erreurs spécifiques et générales sont précisés. Le format correspondant est le suivant :

<Named ClientSI: Report> :: = <[<GPERR>] *(<report>)>
<report> :: = <ErrorPRID> <CPERR> *(<PRID><EPD>)

Typiquement, les rapports de type « Accounting » renferment des données statistiques ou de l'information liée à un événement, toutes deux se rapportant à la configuration installée au niveau du PEP. Le format est comme suit :

<Named ClientSI: Report> :: = <*(<PRID><EPD>)>

A.8 Module 3GPP Go PIB

A.8.1 Précision sur l'objet *Context*

Cet objet est inclus dans les messages COPS-Req et COPS-Dec. Il précise l'événement déclencheur. L'extension 3GPP Go PIB ajoute des valeurs spécifiques au type de client (*Client-Specific*). Noter que le drapeau pour le type de requête demeure de type configuration (0x08). Le format est montré à la Figure A.18.

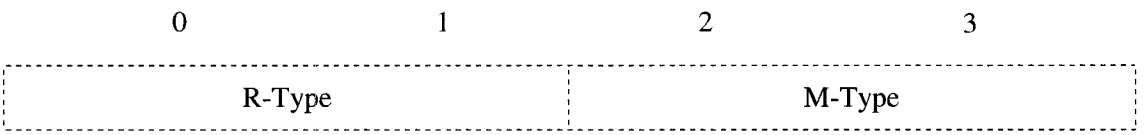

Figure A.18 Format de l'objet *Context* de 3GPP

R-Type (*Request type flag*)		M-Type (*Message type flag*)	
0x08	Requête de configuration	0x01	Négociation initiale des aptitudes
		0x02	Créer un état pour l'événement
		0x03	Mettre à jour l'état pour l'événement
		0x04	Mettre fin à l'état pour l'événement

A.8.2 Module 3GPP Go PIB (3GPP TS 29.207 v5.4.0)

```
GO3GPP-PIB  PIB-DEFINITIONS ::= BEGIN

   IMPORTS
       Unsigned32, Integer32, MODULE-IDENTITY,
       MODULE-COMPLIANCE, OBJECT-TYPE, OBJECT-GROUP
               FROM COPS-PR-SPPI            -- Defined in RFC 3159 [9]
       InstanceId, Prid
               FROM COPS-PR-SPPI-TC         -- Defined in RFC 3159 [9]
       zeroDotZero               FROM SNMPv2-SMI

       InetAddress, InetAddressType,
       InetAddressPrefixLength
               FROM INET-ADDRESS-MIB;       -- Defined in RFC 3291 [19]


   go3gppPib  MODULE-IDENTITY
       SUBJECT-CATEGORIES   { go3gpp (0x8009) } -- Go 3GPP COPS Client Type

       LAST-UPDATED "200305240000Z"
       ORGANIZATION "3GPP TSG CN WG3"
       CONTACT-INFO
                    "Kwok Ho Chan
                     Nortel Networks
                     600 Technology Park Drive
                     Billerica, MA 01821 USA
                     Phone: +1 978 288 8175
                     Email: khchan@nortelnetworks.com

                     Louis-Nicolas Hamer
                     Nortel Networks
                     PO Box 3511 Station C
                     Ottawa, Ontario
                     Canada, K1Y 4H7
                     Phone: +1 613 768 3409
                     Email: nhamer@nortelnetworks.com"
       DESCRIPTION
               "A PIB module containing the set of provisioning
               classes that are required for support of policies for
               3GPP's GO interface, Release 5."
       REVISION "200305240000Z "
       DESCRIPTION
               "The 3GPP Go PIB for release 5
                Annex B of 3GPP TS 29.207 v5.4.0."

          ::= { 1 3 6 1 4 1 10415 1 1  } --  full specification of object ID tree.
                                         -- The final syntax should be { 3gpp_pib 1 }
                                         -- With imports from the document that shows
                                         -- that 3gpp_pib means ( 1.3.6.1.4.1.10415.1 )


--
-- The root OID for PRCs in the 3GPP GO PIB
--

   go3gppCapabilityClasses      OBJECT IDENTIFIER ::= { go3gppPib 1 }
   go3gppEventHandlerClasses    OBJECT IDENTIFIER ::= { go3gppPib 2 }
   go3gppEventClasses           OBJECT IDENTIFIER ::= { go3gppPib 3 }
   go3gppEventInfoClasses       OBJECT IDENTIFIER ::= { go3gppPib 4 }
   go3gppReqInfoClasses         OBJECT IDENTIFIER ::= { go3gppEventInfoClasses 1 }
   go3gppDecInfoClasses         OBJECT IDENTIFIER ::= { go3gppEventInfoClasses 2 }
   go3gppReportClasses          OBJECT IDENTIFIER ::= { go3gppPib 5 }
   go3gppConformance            OBJECT IDENTIFIER ::= { go3gppPib 6 }
-- ------------------------------------------------------------
```

```
--
-- Capability and Limitation Policy Rule Classes
--

--
-- 3GPP GO Capability Table
--

   go3gppAuthReqCapTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppAuthReqCapEntry
       PIB-ACCESS      notify
       STATUS          current
       DESCRIPTION
           "The 3GPP Go Authorization Request Capability PRC."
       ::= { go3gppCapabilityClasses 1 }


   go3gppAuthReqCapEntry OBJECT-TYPE
       SYNTAX          Go3gppAuthReqCapEntry
       STATUS          current
       DESCRIPTION
           "An instance of the go3gppAuthReqCap class identifies a
           specific PRC and associated attributes as supported
           by the device."

       PIB-INDEX { go3gppAuthReqCapPrid }
       UNIQUENESS { }
       ::= { go3gppAuthReqCapTable 1 }


   Go3gppAuthReqCapEntry ::= SEQUENCE {
           go3gppAuthReqCapPrid          InstanceId,
           go3gppAuthReqCapBindingInfos  Unsigned32,
           go3gppAuthReqCapFlowIds       Unsigned32
   }


   go3gppAuthReqCapPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of the go3gppAuthReqCap class."
       ::= { go3gppAuthReqCapEntry 1 }


   go3gppAuthReqCapBindingInfos OBJECT-TYPE
       SYNTAX          Unsigned32
       STATUS          current
       DESCRIPTION
           "Indication of the maximum number of Binding Information
           the PEP can send with each Authorization Request.
           The value of zero indicates limit is not specified."
       DEFVAL  { 0 }
       ::= { go3gppAuthReqCapEntry 2 }


   go3gppAuthReqCapFlowIds OBJECT-TYPE
       SYNTAX          Unsigned32
       STATUS          current
       DESCRIPTION
           "Indication of the maximum number of Flow identifiers the PEP can
           send with each Authorization Request.
           The value of zero indicates limit is not specified."
       DEFVAL  { 0 }
       ::= { go3gppAuthReqCapEntry 3 }
--
```

```
-- Go 3GPP Authorization Request Decision Capabilities
--

   go3gppAuthReqDecCapTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppAuthReqDecCapEntry
       PIB-ACCESS      notify
       STATUS          current
       DESCRIPTION
           "The 3GPP Go Authorization Request Decision Capability PRC."
       ::= { go3gppCapabilityClasses 2 }


   go3gppAuthReqDecCapEntry OBJECT-TYPE
       SYNTAX          Go3gppAuthReqDecCapEntry
       STATUS          current
       DESCRIPTION
           "An instance of the go3gppAuthReqDecCap class identifies a
           specific PRC and associated attributes as supported
           by the device."

       PIB-INDEX { go3gppAuthReqDecCapPrid }
       UNIQUENESS { }
       ::= { go3gppAuthReqDecCapTable 1 }


   Go3gppAuthReqDecCapEntry ::= SEQUENCE {
           go3gppAuthReqDecCapPrid           InstanceId,
           go3gppAuthReqDecCapIcids          Unsigned32
   }

   go3gppAuthReqDecCapPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of the go3gppAuthReqDecCap class."
       ::= { go3gppAuthReqDecCapEntry 1 }

   go3gppAuthReqDecCapIcids OBJECT-TYPE
       SYNTAX          Unsigned32
       STATUS          current
       DESCRIPTION
           "Indication of the maximum number of Icid possible
           in a single Authorization Request Decision.
           The value of zero indicates limit is not specified."
       DEFVAL  { 0 }
       ::= { go3gppAuthReqDecCapEntry 2 }


--
-- Component Limitations Table
--
-- This table supports the ability to export information
-- detailing provisioning class/attribute implementation limitations
-- to the policy decision function. This Component Limitiations Table
-- shall be implementation dependant and does not need to be standardized.


-- ------------------------------------------------------------
--
-- 3GPP GO Event Handler Provisioning Classes
--
-- PRCs sent from PDF to PEP for indicating how to handle each
-- kind of event that require actions by the GO interface.
--
-- For 3GPP Release 5, PRCs for Event Handling of Authorization Request containing
-- Binding Information, Flow identifiers, and QoS is specified.
```

```
--
-- 3GPP GO Authorization Request Event Handler Provisioning Table
--

   go3gppAuthReqHandlerTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppAuthReqHandlerEntry
       PIB-ACCESS      install
       STATUS          current
       DESCRIPTION
           "PRC from PDF to PEP carried by COPS DEC messages
           indicating GO actions to take at the GGSN when an Authorization
           Request Event is detected by the GGSN.  An example of an
           Authorization Request Event is the receive of a PDP Context message."
       ::= { go3gppEventHandlerClasses 1 }


   go3gppAuthReqHandlerEntry OBJECT-TYPE
       SYNTAX          Go3gppAuthReqHandlerEntry
       STATUS          current
       DESCRIPTION
           "An instance of the go3gppAuthReqHandler class sent by the PDF to
           the PEP what the PEP should send upon detection of an Authorization
           Request Event."
       PIB-INDEX { go3gppAuthReqHandlerPrid }
       UNIQUENESS { go3gppAuthReqHandlerEnable,
                    go3gppAuthReqHandlerBindingInfo
                  }
       ::= { go3gppAuthReqHandlerTable 1 }


   Go3gppAuthReqHandlerEntry ::= SEQUENCE {
           go3gppAuthReqHandlerPrid         InstanceId,
           go3gppAuthReqHandlerEnable       INTEGER,
           go3gppAuthReqHandlerBindingInfo  Unsigned32
   }


   go3gppAuthReqHandlerPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of this class."
       ::= { go3gppAuthReqHandlerEntry 1 }


   go3gppAuthReqHandlerEnable OBJECT-TYPE
       SYNTAX          INTEGER {
                           enable(1),
                           disable(2)
                       }
       STATUS          current
       DESCRIPTION
           "Controls the usage of 3GPP Authorization Request Events
           to trigger COPS requests to PDF on the go interface."
       DEFVAL { enable }
       ::= { go3gppAuthReqHandlerEntry 2 }


   go3gppAuthReqHandlerBindingInfo OBJECT-TYPE
       SYNTAX          Unsigned32
       STATUS          current
       DESCRIPTION
           "Indication of the maximum number of Binding Information
           be associated with a each Authorizating Request.
           The value of zero indicates policy control does not impose
           any limit."
```

```
        DEFVAL  { 0 }
        ::= { go3gppAuthReqHandlerEntry 3 }


-- ------------------------------------------------------------
--
-- 3GPP GO Event Classes
--
-- PRCs from PEP to PDF carried by COPS REQ messages
-- indicating the detection of specific events in the GGSN.
-- Information required for PDF to make decision on behave
-- of GGSN is also defined here to be carried by REQ messages.
--

--
-- 3GPP GO Authorization Request Event Table
--
    go3gppAuthReqEventTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppAuthReqEventEntry
        PIB-ACCESS      notify
        STATUS          current
        DESCRIPTION
            "PRC for indication of Authorization Request Event
            and its relevant information.
            Sent by PEP to PDF upon receive of an Authorization
            Request.  Using COPS REQ message."
        ::= { go3gppEventClasses 1 }


    go3gppAuthReqEventEntry OBJECT-TYPE
        SYNTAX          Go3gppAuthReqEventEntry
        STATUS          current
        DESCRIPTION
            "An entry in the Authorization Request Event Table
            describe a single Event sent by the PEP to the PDF."
        PIB-INDEX { go3gppAuthReqEventPrid }
        UNIQUENESS { }
        ::= { go3gppAuthReqEventTable 1 }


    Go3gppAuthReqEventEntry ::= SEQUENCE {
            go3gppAuthReqEventPrid          InstanceId,
            go3gppAuthReqEventBindingInfos Prid
    }


    go3gppAuthReqEventPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppAuthReqEvent class."
        ::= { go3gppAuthReqEventEntry 1 }


    go3gppAuthReqEventBindingInfos OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the first of a list of go3gppBindingInfo
            class instances that are associated with this
            Authorization Request Event.
            A value of zeroDotZero indicates there are no
            go3gppBindingInfo class instance associated with
            this Authorization Event."
        ::= { go3gppAuthReqEventEntry 2 }
```

```
--
-- 3GPP Go Event Request Info Classes
--

--
-- 3GPP GO Binding Information Table
--
   go3gppBindingInfoTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppBindingInfoEntry
       PIB-ACCESS      notify
       STATUS          current
       DESCRIPTION
           "PRC representing Binding Information.
           Sent by PEP to PDF as part of an Authorization
           Request.  In a COPS REQ message."
       ::= { go3gppReqInfoClasses 1 }


   go3gppBindingInfoEntry OBJECT-TYPE
       SYNTAX          Go3gppBindingInfoEntry
       STATUS          current
       DESCRIPTION
           "An entry in the Binding Information Table
           describing a single Binding Info.
           Each entry is referenced by go3gppAuthReqEventBindingInfos
           or go3gppBindingInfoNext."
       PIB-INDEX { go3gppBindingInfoPrid }
       UNIQUENESS { }
       ::= { go3gppBindingInfoTable 1 }


   Go3gppBindingInfoEntry ::= SEQUENCE {
           go3gppBindingInfoPrid           InstanceId,
           go3gppBindingInfoToken          OCTET STRING,
           go3gppBindingInfoFlowIds        Prid,
           go3gppBindingInfoNext           Prid
   }


   go3gppBindingInfoPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of the go3gppBindingInfo class."
       ::= { go3gppBindingInfoEntry 1 }


   go3gppBindingInfoToken OBJECT-TYPE
       SYNTAX          OCTET STRING
       STATUS          current
       DESCRIPTION
           "The Authorization Token associated with this
           instance of the go3gppBindingInfo class.
           Each Binding Information must have a Token."
       ::= { go3gppBindingInfoEntry 2 }


   go3gppBindingInfoFlowIds OBJECT-TYPE
       SYNTAX          Prid
       STATUS          current
       DESCRIPTION
           "References the first of a list of FlowIds associated
           with this instance of go3gppBindingInfo class.
           This is the anchor of a list of go3gppFlowIdEntry Instances.
           A value of zeroDotZero indicates an empty list which
           is an error condition."
```

```
        DEFVAL  { zeroDotZero }
        ::= { go3gppBindingInfoEntry 3 }


    go3gppBindingInfoNext OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the next of a list of go3gppBindingInfo
            instances associated with an Authorization Request.
            A value of zeroDotZero indicates this is the last of
            a list of go3gppBindingInfo instances associated with
            an Authorization Request."
        DEFVAL  { zeroDotZero }
        ::= { go3gppBindingInfoEntry 4 }


--
-- 3GPP Go Authorization Request FlowID Table
--
    go3gppFlowIdTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppFlowIdEntry
        PIB-ACCESS      notify
        STATUS          current
        DESCRIPTION
            "Represents the collection of FlowIDs."
        ::= { go3gppReqInfoClasses 2 }


    go3gppFlowIdEntry OBJECT-TYPE
        SYNTAX          Go3gppFlowIdEntry
        STATUS          current
        DESCRIPTION
            "Each entry describes a single FlowID."
        PIB-INDEX { go3gppFlowIdPrid }
        UNIQUENESS { }
        ::= { go3gppFlowIdTable 1 }


    Go3gppFlowIdEntry ::= SEQUENCE {
            go3gppFlowIdPrid          InstanceId,
            go3gppFlowIdFlowId        Unsigned32,
            go3gppFlowIdNext          Prid
    }


    go3gppFlowIdPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppFlowId class."
        ::= { go3gppFlowIdEntry 1 }


    go3gppFlowIdFlowId OBJECT-TYPE
        SYNTAX          Unsigned32
        STATUS          current
        DESCRIPTION
            "The FlowId itself."
        ::= { go3gppFlowIdEntry 2 }


    go3gppFlowIdNext OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
```

```
            "References the next FlowId in the list associated with the
            same Binding Information of an Authorization Request.
            This points to a list of go3gppFlowIdEntry Instances.
            A value of zeroDotZero indicates end of the list."
        DEFVAL  { zeroDotZero }
        ::= { go3gppFlowIdEntry 3 }


-- ------------------------------------------------------------
--
-- 3GPP Go Authorization Request Decisions
--
-- PRCs for carrying the Event Decision send from PDF to PEP,
-- carried by the COPS DEC message.
-- These PRCs include support for Gates/Filters, QoS, ICIDs.
--

-- Failure Decisions can be defined by use of COPS-PR DEC message
-- containing first an install decision (with objects indicating
-- what failed and some indication to the GGSN how to react to this
-- Error Decision), and second a remove decision (for cleanup of
-- the installed Error Decision Object).
--

-- Failures indicated by PDF to GGSN
--   Authorization Failure
--
--
-- Authorization Request Failure Decision Table
--
    go3gppAuthReqFailDecTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppAuthReqFailDecEntry
        PIB-ACCESS      install
        STATUS          current
        DESCRIPTION
            "The Authorization failure Table. Indicates failures decisions to the PEP."
        ::= { go3gppDecInfoClasses 1 }


    go3gppAuthReqFailDecEntry OBJECT-TYPE
        SYNTAX          Go3gppAuthReqFailDecEntry
        STATUS          current
        DESCRIPTION
            "Each go3gppAuthReqFailDecEntry is per request."
        PIB-INDEX { go3gppAuthReqFailDecPrid }
        UNIQUENESS { }
        ::= { go3gppAuthReqFailDecTable 1 }


    Go3gppAuthReqFailDecEntry ::= SEQUENCE {
            go3gppAuthReqFailDecPrid        InstanceId,

            go3gppAuthReqFailDecReason      INTEGER
    }

    go3gppAuthReqFailDecPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppAuthReqFailDec class."
        ::= { go3gppAuthReqFailDecEntry 1 }


    go3gppAuthReqFailDecReason OBJECT-TYPE
        SYNTAX          INTEGER {
                          noCorrespondingSession (1),
```

```
                    invalidBundling (2),
                    authorizationFailure (3)
                  }
      STATUS        current
      DESCRIPTION
          "Reason for Auth Request Failure Decision given by PDF:

           noCorrespondingSession:  No corresponding session was found by the PDF

           invalidBundling:         In case the UE violates the IMS level indication
                                    and attempts to set up multiple IMS media
                                    components in a single PDP context despite of an
                                    indication that mandated separate PDP contexts or
                                    if the list of flow identifiers contained in the
                                    bearer authorization request doesn't match with
                                    the grouping indication information the PDF has
                                    received from the P-CSCF.
           authorizationFailure:    The PDF is unable to authorise the binding
                                    information.  This is a generic failure
                                    indication that can be used if the actual reason
                                    is not any of the other specified reasons."

      ::= { go3gppAuthReqFailDecEntry 2 }


--
-- Authorization Request Decision Table
--
   go3gppAuthReqDecTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppAuthReqDecEntry
       PIB-ACCESS      install
       STATUS          current
       DESCRIPTION
           "The Authorization Request Decision Table. "
       ::= { go3gppDecInfoClasses 2 }


   go3gppAuthReqDecEntry OBJECT-TYPE
       SYNTAX          Go3gppAuthReqDecEntry
       STATUS          current
       DESCRIPTION
           "Each go3gppAuthReqDecEntry is per Authorization Request."
       PIB-INDEX { go3gppAuthReqDecPrid }
       UNIQUENESS { }
       ::= { go3gppAuthReqDecTable 1 }
   Go3gppAuthReqDecEntry ::= SEQUENCE {
           go3gppAuthReqDecPrid       InstanceId,
           go3gppAuthReqDecIcids      Prid,
           go3gppAuthReqDecDirDecs    Prid
   }


   go3gppAuthReqDecPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of the go3gppAuthReqDec class."
       ::= { go3gppAuthReqDecEntry 1 }


   go3gppAuthReqDecIcids OBJECT-TYPE
       SYNTAX          Prid
       STATUS          current
       DESCRIPTION
           "References the first of a list of IcIDs associated
           with this instance of go3gppAuthReqDec class.
```

```
            There should be one IcID on this list for each Binding
            Information in the corresponding Authorization Request.
            A value of zeroDotZero indicates an empty list and there
            is no IcID change associated with this Authorization Request
            Decision."
        DEFVAL  { zeroDotZero }
        ::= { go3gppAuthReqDecEntry 2 }


    go3gppAuthReqDecDirDecs OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the first of a list of Directional Decisions
            associated with this instance of go3gppAuthReqDec class.
            There should be at least one and at most two Directional
            Decisions per Authorization Request Decision.
            Hence a value of zeroDotZero is illegal."
        ::= { go3gppAuthReqDecEntry 3 }


--
-- 3GPP Go ICID Table
--
    go3gppIcidTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppIcidEntry
        PIB-ACCESS      install
        STATUS          current
        DESCRIPTION
            "Represents the collection of ICID entries"
        ::= { go3gppDecInfoClasses 3 }


    go3gppIcidEntry OBJECT-TYPE
        SYNTAX          Go3gppIcidEntry
        STATUS          current
        DESCRIPTION
            "Represents the ICID Entry"
        PIB-INDEX { go3gppIcidPrid }
        UNIQUENESS { go3gppIcidValue }
        ::= { go3gppIcidTable 1 }


    Go3gppIcidEntry ::= SEQUENCE {
            go3gppIcidPrid              InstanceId,
            go3gppIcidValue             OCTET STRING,
            go3gppIcidNext              Prid
    }


    go3gppIcidPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppIcid class."
        ::= { go3gppIcidEntry 1 }


    go3gppIcidValue OBJECT-TYPE
        SYNTAX          OCTET STRING
        STATUS          current
        DESCRIPTION
            "The ICID itself. "
        ::= { go3gppIcidEntry 2 }
```

```
    go3gppIcidNext OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the next go3gppIcidEntry of a list of ICIDs
            associated with this instance of go3gppAuthReqDec class.
            There should be one ICID on this list for each Binding
            Information in the corresponding Authorization Request.
            A value of zeroDotZero indicates the end of the list of
            ICIDs associated with an Authorization Request Decision."
        DEFVAL  { zeroDotZero }
        ::= { go3gppIcidEntry 3 }


--
-- 3GPP Go Authorization Request Directional Decision Table
--
    go3gppAuthReqDirDecTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppAuthReqDirDecEntry
        PIB-ACCESS      install
        STATUS          current
        DESCRIPTION
            "This table represents the authorization request decision for
             unique direction (e.g. uplink and downlink)."
        ::= { go3gppDecInfoClasses 4 }


    go3gppAuthReqDirDecEntry OBJECT-TYPE
        SYNTAX          Go3gppAuthReqDirDecEntry
        STATUS          current
        DESCRIPTION
            "There should be one of these per direction per AuthReqDec."
        PIB-INDEX { go3gppAuthReqDirDecPrid }
        UNIQUENESS { }
        ::= { go3gppAuthReqDirDecTable 1 }


    Go3gppAuthReqDirDecEntry ::= SEQUENCE {
            go3gppAuthReqDirDecPrid      InstanceId,
            go3gppAuthReqDirDecDirection INTEGER,
            go3gppAuthReqDirDecQos       Prid,
            go3gppAuthReqDirDecGates     Prid,
            go3gppAuthReqDirDecNext      Prid
    }

    go3gppAuthReqDirDecPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppAuthReqDirDec class."
        ::= { go3gppAuthReqDirDecEntry 1 }


    go3gppAuthReqDirDecDirection OBJECT-TYPE
        SYNTAX          INTEGER {
                            uplink   (1),
                            downlink (2)
                        }
        STATUS          current
        DESCRIPTION
            "Indicates the direction this decision applies to."
        ::= { go3gppAuthReqDirDecEntry 2 }


    go3gppAuthReqDirDecQos OBJECT-TYPE
        SYNTAX          Prid
```

```
        STATUS          current
        DESCRIPTION
            " The Authorized QoS. References the go3gppQos class."
        ::= { go3gppAuthReqDirDecEntry 3 }


    go3gppAuthReqDirDecGates OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the first instance of a list of the go3gppGate class."
        ::= { go3gppAuthReqDirDecEntry 4 }


    go3gppAuthReqDirDecNext OBJECT-TYPE
        SYNTAX          Prid
        STATUS          current
        DESCRIPTION
            "References the next instance of a list of
            go3gppAuthReqDirDec class."
        ::= { go3gppAuthReqDirDecEntry 5 }


--
-- 3GPP Go QoS Table
--
    go3gppQosTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppQosEntry
        PIB-ACCESS      install
        STATUS          current
        DESCRIPTION
            "This table represents the Authorised QoS.
            It is referenced by the go3gppAuthReqDirDecQos entry of the
            go3gppAuthReqDirDecEntry  class."
        ::= { go3gppDecInfoClasses 5 }


    go3gppQosEntry OBJECT-TYPE
        SYNTAX          Go3gppQosEntry
        STATUS          current
        DESCRIPTION
            "There should be one of these per direction per AuthReqDec."
        PIB-INDEX { go3gppQosPrid }
        UNIQUENESS { }
        ::= { go3gppQosTable 1 }


    Go3gppQosEntry ::= SEQUENCE {
            go3gppQosPrid               InstanceId,
            go3gppQosServiceClass       INTEGER,
            go3gppQosDataRateUnit       INTEGER,
            go3gppQosDataRate           Unsigned32
    }


    go3gppQosPrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gppQos class."
        ::= { go3gppQosEntry 1 }


    go3gppQosServiceClass OBJECT-TYPE
        SYNTAX          INTEGER {
```

```
                        qosclassA     (1),
                        qosclassB     (2),
                        qosclassC     (3),
                        qosclassD     (4),
                        qosclassE     (5),
                        qosclassF     (6)
                      }
    STATUS            current
    DESCRIPTION
        "The QoS Service Class indicates the highest authorized QoS class."
    ::= { go3gppQosEntry 2 }


go3gppQosDataRateUnit OBJECT-TYPE
    SYNTAX            INTEGER {
                        bps     (1),
                        kbps    (2),
                        mbps    (3)
                      }
    STATUS            current
    DESCRIPTION
        "Indication of the unit of measure for go3gppQosDataRate,
         in bits per second, kilo bits per second, or mega bits per
         second."
    ::= { go3gppQosEntry 3 }


go3gppQosDataRate OBJECT-TYPE
    SYNTAX            Unsigned32
    STATUS            current
    DESCRIPTION
        "The Data Rate with unit of measure indicated by
        go3gppQosDataRateUnit."
    ::= { go3gppQosEntry 4 }


--
-- 3GPP Go Gate Decision Table
--
--
-- There could be one of these per direction per GateDec.
--
-- This is for changing Gating Status only when used alone
-- (not as part of Direction Decision).

-- go3gppGateDec is sent in a different COPS DEC message
-- from the DEC message carrying go3gppAuthReqDec. PDF must
-- have sent a go3gppAuthReqDec before using go3gppGateDec.

go3gppGateDecTable OBJECT-TYPE
    SYNTAX            SEQUENCE OF Go3gppGateDecEntry
    PIB-ACCESS        install
    STATUS            current
    DESCRIPTION
        "This table represents an updated gating decision."
    ::= { go3gppDecInfoClasses 6 }


go3gppGateDecEntry OBJECT-TYPE
    SYNTAX            Go3gppGateDecEntry
    STATUS            current
    DESCRIPTION
        "There should be one of these per direction per AuthReqDec."
    PIB-INDEX { go3gppGateDecPrid }
    UNIQUENESS { }
    ::= { go3gppGateDecTable 1 }
```

```
  Go3gppGateDecEntry ::= SEQUENCE {
        go3gppGateDecPrid           InstanceId,
        go3gppGateDecDirection      INTEGER,
        go3gppGateDecGates          Prid,
        go3gppGateDecNext           Prid
}

go3gppGateDecPrid OBJECT-TYPE
    SYNTAX          InstanceId
    STATUS          current
    DESCRIPTION
        "An arbitrary integer index that uniquely identifies an
        instance of the go3gppGateDec class."
    ::= { go3gppGateDecEntry 1 }

go3gppGateDecDirection OBJECT-TYPE
    SYNTAX          INTEGER {
                        uplink   (1),
                        downlink (2)
                    }
    STATUS          current
    DESCRIPTION
        "References the gate direction."
    ::= { go3gppGateDecEntry 2 }

 go3gppGateDecGates OBJECT-TYPE
    SYNTAX          Prid
    STATUS          current
    DESCRIPTION
        "References the first instance of a list of go3gppGate class."
    ::= { go3gppGateDecEntry 3 }

go3gppGateDecNext OBJECT-TYPE
    SYNTAX          Prid
    STATUS          current
    DESCRIPTION
        "References the next instance of a list of go3gppGateDec class."
    ::= { go3gppGateDecEntry 4 }

--
-- 3GPP Go Gate Table
--
go3gppGateTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Go3gppGateEntry
    PIB-ACCESS      install
    STATUS          current
    DESCRIPTION
        "PRC representing a Gate."
    ::= { go3gppDecInfoClasses 7 }

go3gppGateEntry OBJECT-TYPE
    SYNTAX          Go3gppGateEntry
    STATUS          current
    DESCRIPTION
        "Each instance represents one Gate."
    PIB-INDEX { go3gppGatePrid }
    UNIQUENESS { }
    ::= { go3gppGateTable 1 }

Go3gppGateEntry ::= SEQUENCE {
        go3gppGatePrid              InstanceId,
```

```
        go3gppGateFilter            Prid,
        go3gppGateStatus            INTEGER,
        go3gppGateNext              Prid
}


go3gppGatePrid OBJECT-TYPE
    SYNTAX          InstanceId
    STATUS          current
    DESCRIPTION
        "An arbitrary integer index that uniquely identifies an
        instance of the go3gppGate class."
    ::= { go3gppGateEntry 1 }


go3gppGateFilter OBJECT-TYPE
    SYNTAX          Prid
    STATUS          current
    DESCRIPTION
        "References an entry in frwkIpFilterTable (Framework PIB)
        that describes the applicable classification filter.

        When a decision requiring the definition of an IP filter
        is sent to the GGSN, the IP filter will be represented by the
        IP filter definition frwkIpFilterTable, provided by the
        Framework PIB, RFC 3318. Such IP filter frwkIpFilterTable
        must be part of the same decision message. The attribute
        go3gppGateFilter is used to reference the frwkIpFilterTable
        entry for this Gate.
        Wildcarding of the attributes for deriving the address and protocol values
        is as specified in RFC 3318 [15]. Wildcarding of the source ports is achieved
as follows:
        - frwkIpFilterSrcL4PortMin shall be set to 0,
        - and frwkIpFilterSrcL4PortMax shall be set to 65535

        The frwkBaseFilterNegation attribute of the frwkBaseFilterTable is
        not required, its "not-used" condition is indicated by setting its
        value to "false".

        The frwkIpFilterDscp and frwkIpFilterFlowId attributes
        of the frwkIpFilterTable are not required, their "not-used" condition is
        indicated by setting their values to -1.

        A value of zeroDotZero indicates no filter is
        used with this go3gppGate."
    ::= { go3gppGateEntry 2 }

go3gppGateStatus OBJECT-TYPE

    SYNTAX          INTEGER {
                        close   (1),
                        open    (2)
                    }
    STATUS          current
    DESCRIPTION
        "Indicates if this gate will allow traffic to flow."
 DEFVAL  { close }
    ::= { go3gppGateEntry 3 }

go3gppGateNext OBJECT-TYPE
    SYNTAX          Prid
    STATUS          current
    DESCRIPTION
        "Reference the next Gate on a list of go3gppGate instances.
        A value of zeroDotZero indicates this is the last Gate
        on the list."
```

```
        ::= { go3gppGateEntry 4 }

-- ------------------------------------------------------------
--
-- 3GPP Go Reports
--
-- PRCs for carrying the Decision enforcement result sent from PEP to PDF,
-- carried using the COPS REPORT message.
-- These PRCs include support for the success or failure of the PEP in
-- carrying out the PDF's decision or -change of the state in the GGSN.
--

   go3gppReportTable OBJECT-TYPE
       SYNTAX          SEQUENCE OF Go3gppReportEntry
       PIB-ACCESS      notify
       STATUS          current
       DESCRIPTION
           "This table represents the success or failure of the decision enforcement and
           state changes in the PEP."
       ::= { go3gppReportClasses 1 }


   go3gppReportEntry OBJECT-TYPE
       SYNTAX          Go3gppReportEntry
       STATUS          current
       DESCRIPTION
           ""
       PIB-INDEX { go3gppReportPrid }
       UNIQUENESS { }
       ::= { go3gppReportTable 1 }


   Go3gppReportEntry ::= SEQUENCE {
           go3gppReportPrid        InstanceId,
           go3gppReportStatus      INTEGER,
           go3gppReportDetails     Prid
   }
   go3gppReportPrid OBJECT-TYPE
       SYNTAX          InstanceId
       STATUS          current
       DESCRIPTION
           "An arbitrary integer index that uniquely identifies an
           instance of the go3gpgReport class."
           ::= { go3gppReportEntry 1 }


   go3gppReportStatus OBJECT-TYPE
       SYNTAX          INTEGER {
                               success (1),
                               failure (2),
                               usage   (3) }
       STATUS          current
       DESCRIPTION
           "When Status is:
              success: Indicates the successful implementation of the
                       decision.
                       go3gppReportDetails:
                         Reference an instance of go3gppRprtGPRSChrgInfo
                         for initial authorization request decision;
                         References nothing otherwise (contains the value
                         zeroDotZero).

              Failure: Indicates the failure of implementing the decision.

                       go3gppReportDetails may references an Error object,
                       or may have the value zeroDotZero when no error
                       object is needed, in which case COPS and COPS-PR
```

```
                error codes and error objects are sufficient.
        Usage:  go3gppReportDetails references an instance of
                go3gppRprtUsage class."

    ::= { go3gppReportEntry 2 }


go3gppReportDetails OBJECT-TYPE
    SYNTAX          Prid
    STATUS          current
    DESCRIPTION
        "May reference an instance of go3gppRprtGPRSChrgInfo,
        go3gppRprtError(not defined), or go3gppRprtUsage class,
        or may have the value of zeroDotZero depending on the value of
        go3gppReportStatus."
    ::= { go3gppReportEntry 3 }


go3gppRprtGPRSChrgInfoTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Go3gppRprtGPRSChrgInfoEntry
    PIB-ACCESS      notify
    STATUS          current
    DESCRIPTION
        "This table represents the GPRS Charging information"
    ::= { go3gppReportClasses 2 }


go3gppRprtGPRSChrgInfoEntry OBJECT-TYPE
    SYNTAX          Go3gppRprtGPRSChrgInfoEntry
    STATUS          current
    DESCRIPTION
        "This entry represents the GPRS Charging Identifier and GGSN address."
    PIB-INDEX { go3gppRprtGPRSChrgInfoPrid }
    UNIQUENESS { go3gppRprtGPRSChrgInfoAddrType,
                 go3gppRprtGPRSChrgInfoGGSNAddr,
                 go3gppRprtGPRSChrgInfoGCID }
    ::= { go3gppRprtGPRSChrgInfoTable 1 }
Go3gppRprtGPRSChrgInfoEntry ::= SEQUENCE {
        go3gppRprtGPRSChrgInfoPrid        InstanceId,

        go3gppRprtGPRSChrgInfoAddrType    InetAddressType,

        go3gppRprtGPRSChrgInfoGGSNAddr    InetAddress,
        go3gppRprtGPRSChrgInfoGCID        OCTET STRING
}


go3gppRprtGPRSChrgInfoPrid OBJECT-TYPE
    SYNTAX          InstanceId
    STATUS          current
    DESCRIPTION
        "An arbitrary integer index that uniquely identifies an
        instance of the go3gpgRprtGPRSChrgInfo class."
        ::= { go3gppRprtGPRSChrgInfoEntry 1 }

go3gppRprtGPRSChrgInfoAddrType OBJECT-TYPE
    SYNTAX          InetAddressType
    STATUS          current
    DESCRIPTION
        "The address type enumeration value to specify
         the type of the packet's IP address."
    REFERENCE
        "Textual Conventions for Internet Network Addresses [INETADDR]."
    ::= { go3gppRprtGPRSChrgInfoEntry 2 }

go3gppRprtGPRSChrgInfoGGSNAddr OBJECT-TYPE
    SYNTAX          InetAddress
```

```
        STATUS          current
        DESCRIPTION
            "Contains the IP Address of the GGSN providing the GCID
            upon successful handling of an Authorization Request."
        REFERENCE
            "Textual Conventions for Internet Network Addresses [INETADDR]."
            ::= { go3gppRprtGPRSChrgInfoEntry 3 }


    go3gppRprtGPRSChrgInfoGCID OBJECT-TYPE
        SYNTAX          OCTET STRING
        STATUS          current
        DESCRIPTION
            "The GPRS Charging ID related to this Authorization Request."
        ::= { go3gppRprtGPRSChrgInfoEntry 4 }


--
-- Notice go3gppRprtError PRC is currently not defined because all
-- error condition handling is satisfactorily covered by using the
-- standard COPS-PR error handling mechanism and error objects.
-- go3gppRprtError PRC should only be used for 3GPP GO Application
-- error indications if necessary.
--

    go3gppRprtUsageTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Go3gppRprtUsageEntry
        PIB-ACCESS      notify
        STATUS          current
        DESCRIPTION
            ""
        ::= { go3gppReportClasses 3 }


    go3gppRprtUsageEntry OBJECT-TYPE
        SYNTAX          Go3gppRprtUsageEntry
        STATUS          current
        DESCRIPTION
            "This entry represents the PEP state changes."
        PIB-INDEX { go3gppRprtUsagePrid }
        UNIQUENESS { go3gppRprtUsageIndication }
        ::= { go3gppRprtUsageTable 1 }


    Go3gppRprtUsageEntry ::= SEQUENCE {
            go3gppRprtUsagePrid         InstanceId,
            go3gppRprtUsageIndication   INTEGER
    }


    go3gppRprtUsagePrid OBJECT-TYPE
        SYNTAX          InstanceId
        STATUS          current
        DESCRIPTION
            "An arbitrary integer index that uniquely identifies an
            instance of the go3gpgRprtUsage class."
            ::= { go3gppRprtUsageEntry 1 }


    go3gppRprtUsageIndication OBJECT-TYPE
        SYNTAX          INTEGER {
                          chngdTo0kbs   (1),
                          chngdFrom0kbs (2) }
        STATUS          current
        DESCRIPTION
            "Indication of GPRS Usage change.
            chngdTo0kbs indicates changing to 0kbs,
```

```
            chngdFrom0kbs indicates changing from 0kbs."
            ::= { go3gppRprtUsageEntry 2 }


-- ------------------------------------------------------------
--
-- Conformance Section
--

   go3gppCompliances          OBJECT IDENTIFIER ::= { go3gppConformance 1 }
   go3gppGroups               OBJECT IDENTIFIER ::= { go3gppConformance 2 }


   go3gppCompliance MODULE-COMPLIANCE
       STATUS  current
       DESCRIPTION
               "Describes the requirements for conformance to the
               3GPP GO PIB."


       MODULE FRAMEWORK-PIB                -- Defined in RFC 3318 [15]
           MANDATORY-GROUPS {
               frwkPrcSupportGroup,
               frwkDeviceIdGroup,
               frwkBaseFilterGroup,
               frwkIpFilterGroup }


       MODULE GO3GPP-PIB -- this module
           MANDATORY-GROUPS {
               go3gppAuthReqCapGroup,
               go3gppAuthReqDecCapGroup,
               go3gppAuthReqHandlerGroup,
               go3gppAuthReqEventGroup,
               go3gppBindingInfoGroup,
               go3gppFlowIdGroup,
               go3gppAuthReqFailDecGroup,
               go3gppAuthReqDecGroup,
               go3gppIcidGroup,
               go3gppAuthReqDirDecGroup,
               go3gppQosGroup,
               go3gppGateDecGroup,
               go3gppGateGroup,
               go3gppReportGroup,
               go3gppRprtGPRSChrgInfoGroup,
               go3gppRprtUsageGroup }
       ::= { go3gppCompliances 1 }


   go3gppAuthReqCapGroup OBJECT-GROUP
       OBJECTS {
       go3gppAuthReqCapBindingInfos,
       go3gppAuthReqCapFlowIds
       }
       STATUS current
       DESCRIPTION
          "This Group defines the PIB Objects that describe the
           Authorization Request capabilities."
       ::= { go3gppGroups 1 }

   go3gppAuthReqDecCapGroup OBJECT-GROUP
       OBJECTS {
       go3gppAuthReqDecCapIcids
       }
       STATUS current
       DESCRIPTION
          "This Group defines the PIB
```

```
        Objects that describe the Authorization Decision capabilities."
    ::= { go3gppGroups 2 }

go3gppAuthReqHandlerGroup OBJECT-GROUP
    OBJECTS {
    go3gppAuthReqHandlerEnable,
    go3gppAuthReqHandlerBindingInfo
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the Authorization request event handler."
    ::= { go3gppGroups 3 }

go3gppAuthReqEventGroup OBJECT-GROUP
    OBJECTS {
    go3gppAuthReqEventBindingInfos
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the Authorization request events."
    ::= { go3gppGroups 4 }

go3gppBindingInfoGroup OBJECT-GROUP
    OBJECTS {
    go3gppBindingInfoToken,
    go3gppBindingInfoFlowIds,
    go3gppBindingInfoNext
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the binding information."
    ::= { go3gppGroups 5 }
go3gppFlowIdGroup OBJECT-GROUP
    OBJECTS {
    go3gppFlowIdFlowId,
    go3gppFlowIdNext
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the flow identifier."
    ::= { go3gppGroups 6 }

go3gppAuthReqFailDecGroup OBJECT-GROUP
    OBJECTS {
    go3gppAuthReqFailDecReason
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the Authorization failure decisions."
    ::= { go3gppGroups 7 }

go3gppAuthReqDecGroup OBJECT-GROUP
    OBJECTS {
    go3gppAuthReqDecIcids,
    go3gppAuthReqDecDirDecs
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the Authorization decisions."
    ::= { go3gppGroups 8 }
```

```
go3gppIcidGroup OBJECT-GROUP
    OBJECTS {
    go3gppIcidValue,
    go3gppIcidNext
    }
    STATUS current
    DESCRIPTION
       "This Group defines the PIB
       Objects that describe the ICID."
    ::= { go3gppGroups 9 }

go3gppAuthReqDirDecGroup OBJECT-GROUP
    OBJECTS {
    go3gppAuthReqDirDecDirection,
    go3gppAuthReqDirDecQos,
    go3gppAuthReqDirDecGates,
    go3gppAuthReqDirDecNext
    }
    STATUS current
    DESCRIPTION
       "This Group defines the PIB
       Objects that describe the authorization decision direction."
    ::= { go3gppGroups 10 }

go3gppQosGroup OBJECT-GROUP
    OBJECTS {
    go3gppQosServiceClass,
    go3gppQosDataRateUnit,
    go3gppQosDataRate
    }
    STATUS current
    DESCRIPTION
       "This Group defines the PIB
       Objects that describe the QoS information."
    ::= { go3gppGroups 11 }
go3gppGateDecGroup OBJECT-GROUP
    OBJECTS {
    go3gppGateDecDirection,
    go3gppGateDecGates,
    go3gppGateDecNext
    }
    STATUS current
    DESCRIPTION
       "This Group defines the PIB
       Objects that describe the Gate decision."
    ::= { go3gppGroups 12 }

go3gppGateGroup OBJECT-GROUP
    OBJECTS {
    go3gppGateFilter,
    go3gppGateStatus,
    go3gppGateNext
    }
    STATUS current
    DESCRIPTION
       "This Group defines the PIB
       Objects that describe the gate."
    ::= { go3gppGroups 13 }


go3gppReportGroup OBJECT-GROUP
    OBJECTS {
    go3gppReportStatus,
    go3gppReportDetails
    }
    STATUS current
    DESCRIPTION
```

```
        "This Group defines the PIB
        Objects that describe the PEP reports."
    ::= { go3gppGroups 14 }

go3gppRprtGPRSChrgInfoGroup OBJECT-GROUP
    OBJECTS {
    go3gppRprtGPRSChrgInfoAddrType,
    go3gppRprtGPRSChrgInfoGGSNAddr,
    go3gppRprtGPRSChrgInfoGCID
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the charging information."
    ::= { go3gppGroups 15 }

go3gppRprtUsageGroup OBJECT-GROUP
    OBJECTS {
    go3gppRprtUsageIndication
    }
    STATUS current
    DESCRIPTION
        "This Group defines the PIB
        Objects that describe the report usage."
    ::= { go3gppGroups 16 }

END
```

A.9 Mises en correspondance

A.9.1 Mises en correspondance dans la fonction de contrôle basée sur des politiques PCF

Tableau A.8 Conversion attributs SDP - attributs QdS IP autorisés par PCF

Maximum Authorized Data Rate DL (Max_DR_DL) and UL (Max_DR_UL) per media component (voir note 1)	IF a=recvonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction:= downlink;
	ELSE /* mobile terminated */
	Direction:= uplink;
	ENDIF;
	ELSE
	IF a=sendonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction: = uplink;
	ELSE /* mobile terminated */
	Direction:= downlink;
	ENDIF;
	ELSE /*sendrecv, inactive or no direction attribute*/
	Direction:=both;
	ENDIF;
	ENDIF;
	
	IF b=AS:<bandwidth> is present THEN
	IF Direction=downlink THEN
	IF <transport>="RTP/AVP" then
	Max_DR_UL:=0.025 * <bandwidth>;
	Max_DR_DL:=1.025 * <bandwidth>;
	ELSE
	Max_DR_UL:=0;
	Max_DR_DL:=<bandwidth>;
	ENDIF;
	ELSE
	IF Direction=uplink THEN
	IF <transport>="RTP/AVP" then
	Max_DR_UL:= 1.025 * <bandwidth>;
	Max_DR_DL:=0.025 * <bandwidth>;
	ELSE
	Max_DR_UL:=<bandwidth>;
	Max_DR_DL:=0;
	ENDIF;
	ELSE /*Direction=both*/
	Max_DR_UL:= 1.025 * <bandwidth>;
	Max_DR_DL:= 1.025 * <bandwidth>;
	ENDIF;
	ENDIF;
	ELSE
	bw:= as set by the operator;
	IF Direction=downlink THEN
	Max_DR_UL:=0;
	Max_DR_DL:=bw;
	ELSE
	IF Direction=uplink THEN
	Max_DR_UL:=bw;
	Max_DR_DL:=0;
	ELSE /*Direction=both*/
	Max_DR_UL:=bw;
	Max_DR_DL:=bw;
	ENDIF; ENDIF; ENDIF;

Tableau A.8 Conversion attributs SDP - attributs QdS IP autorisés par PCF (suite)

Maximum Authorized QoS Class [MaxClass] per media component (notes 2, 3 et 4)	IF (all media components of media type "audio" or "video" for the session are unidirectional and have the same direction) THEN
	MaxClassDerivation:=B; /*streaming*/
	ELSE
	MaxClassDerivation:=A; /*conversational*/
	ENDIF;
	
	CASE <media> OF
	"audio": MaxClass:= MaxClassDerivation
	"video": MaxClass:= MaxClassDerivation
	"application": MaxClass:=A; /*conversational*/
	"data": MaxClass:=E; /*interactive with priority 3*/
	"control": MaxClass:=C; /*interactive with priority 1*/
	/*new media type*/
	OTHERWISE: MaxClass:=F; /*background*/
	END;

NOTE 1: For a RTP media component the Maximum Authorized Data Rates DL/UL are the sum of the Maximum Authorized Data Rates DL/UL for the RTP media streams and the associated RTCP IP flows DL/UL. NOTE 2: The Maximum Authorized QoS Class for a RTCP IP flow is the same as for the corresponding RTP media stream. NOTE 3: When an audio or video stream is removed from a session, the remaining media streams in the session shall keep the originally assigned maximum Authorized QoS classes. NOTE 4: When an audio or video stream is added to a session, the PDF shall derive the maximum Authorized QoS Class taking into account the existing media streams within the session.	

Tableau A.9 Règles du PCF pour les attributs de chaque *Client Handle*

Authorized IP QoS per Client Handle	Calculation Rule

Maximum Authorized Data Rate DL and UL per Client Handle	Maximum Authorized Data Rate DL/UL per Client Handle is the sum of all Maximum Authorized Data Rate DL/UL per media component for all the media component s associated with that Client Handle.
	
	IF Maximum Authorized Data Rate DL/UL per Client Handle > 2 047 kbps THEN
	Maximum Authorized Data Rate DL/UL per Client Handle = 2 047 kbps
	/* See 3GPP TS 23.107 [8] */
	
	END;

Maximum Authorized QoS Class per Client Handle	Maximum Authorized QoS Class per Client Handle = MAX [Maximum Authorized QoS Class per Client Handle among all the media components associated with that Client Handle. (The MAX function ranks the possible Maximum Authorized QoS Class values as follows: "A" > "B" > "C" > "D" > "E" > "F") /* See 3GPP TS 29.207 [7]) */

A.9.2 Mises en correspondance dans l'usager UE

Tableau A.10 Conversion attributs SDP – attributs QdS UMTS dans UE

UMTS QoS Parameter per media component	Derivation from SDP Parameters

Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component	/* Check if the media use codec(s) */
	IF [(<media> = ("audio" or "video")) and (<transport> = "RTP/AVP")]
	THEN
	
	/* Check if Streaming */
	IF a= ("sendonly" or "recvonly") THEN
	Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [5] ;
	/* Conversational as default !*/
	ELSE
	Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [6] ;
	ENDIF ;
	
	/* Check for presence of bandwidth attribute for each media component */
	ELSEIF b=AS:<bandwidth-value> is present THEN
	IF media stream only downlink THEN
	Maximum Bitrate DL = Guaranteed Bitrate DL =<bandwidth>;
	ELSEIF mediastream only uplink THEN
	Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth>;
	ELSEIF mediastreams both downlink and uplink THEN
	Maximum Bitrate DL = Guaranteed Bitrate DL =<bandwidth>;
	Maximum Bitrate UL = Guaranteed Bitrate UL =<bandwidth>;
	ENDIF;
	ELSE
	
	/* SDP do not give any guidance ! */
	Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified by the UE manufacturer;
	ENDIF ;

Tableau A.11 Conversion attributs SDP - attributs QdS UMTS autorisés par UE

Authorized UMTS QoS /media component	Derivation from SDP Parameters

Maximum Authorized Bandwidth DL (Max_BW_DL) and UL (Max_BW_UL) per media component (voir note 3)	IF SBLP is applied THEN
	IF a=recvonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction:= downlink;
	ELSE /* mobile terminated */
	Direction:= uplink;
	ENDIF;
	ELSE;
	IF a=sendonly THEN
	IF <SDP direction> = mobile originated THEN
	Direction: = uplink;
	ELSE /* mobile terminated */
	Direction:= downlink;
	ENDIF;
	ELSE /*sendrecv, inactive or no direction attribute*/
	Direction:=both;
	ENDIF;
	ENDIF;
	IF b=AS:<bandwidth> is present THEN
	IF Direction=downlink THEN
	IF <transport>="RTP/AVP" then
	Max_BW_UL:=0.025 * <bandwidth>;
	Max_BW_DL:=1.025 * <bandwidth>;
	ELSE
	Max_BW_UL:=0;
	Max_BW_DL:=<bandwidth>;
	ENDIF;
	ELSE
	IF Direction=uplink THEN
	IF <transport>="RTP/AVP" then
	Max_BW_UL:= 1.025 * <bandwidth>;
	Max_BW_DL:=0.025 * <bandwidth>;
	ELSE
	Max_BW_UL:=<bandwidth>;
	Max_BW_DL:=0;
	ENDIF;
	ELSE /*Direction=both*/
	Max_BW_UL:= 1.025 * <bandwidth>;
	Max_BW_DL:= 1.025 * <bandwidth>;
	ENDIF;
	ENDIF;
	ELSE
	bw:= as set by the UE manufacturer;
	IF Direction=downlink THEN
	Max_BW_UL:=0;
	Max_BW_DL:= bw;
	ELSE
	IF Direction=uplink THEN
	Max_BW_UL:= bw;
	Max_BW_DL:=0;
	ELSE /*Direction=both*/
	Max_BW_UL:= bw;
	Max_BW_DL:= bw;
	ENDIF;
	ENDIF;
	ENDIF;
	ELSE
	No authorization is done ;
	ENDIF ;

Tableau A.11 Conversion attributs SDP - attributs QdS UMTS autorisés par UE (suite)

Authorized UMTS QoS /media component	Derivation from SDP Parameters

Maximum Authorized Traffic Class [MaxTrafficClass] per media component (voir notes 1, 2 et 4)	IF SBLP is applied THEN
	IF (all media components of media type "audio" or "video" for the session are unidirectional and have the same direction) THEN
	MaxService:= streaming;
	ELSE
	MaxService:= conversational;
	ENDIF;
	
	CASE <media> OF
	"audio": MaxTrafficClass:= MaxService;
	"video": MaxTrafficClass:= MaxService;
	"application": MaxTrafficClass:=conversational;
	"data": MaxTrafficClass:=interactive with priority 3;
	"control": MaxTrafficClass:=interactive with priority 1;
	/*new media type*/
	OTHERWISE: MaxTrafficClass:=background;
	END;
	ELSE
	No authorization is done ;
	ENDIF ;

NOTE 1: When an audio or video stream is removed from a session, the remaining media streams shall keep the originally assigned maximum Authorized Traffic Classes.

NOTE 2: When an audio or video stream is added to a session, the UE shall derive the maximum Authorized TrafficClass taking into account the already existing media streams within the session.

NOTE 3: For a RTP media component the Maximum Authorized Bandwidth DL/UL are the sum of the Maximum Authorized Bandwidths DL/UL for the RTP media streams and the associated RTCP IP flows DL/UL.

NOTE 4: The Maximum Authorized Traffic Class for a RTCP IP flow is the same as for the corresponding RTP media stream.

Tableau A.12 Règles du UE pour déterminer les paramètres de QdS UMTS autorisés de chaque contexte PDP

Authorized UMTS QoS Parameter per PDP Context	Calculation Rule

Maximum Authorized Bandwidth DL and UL per PDP Context	IF SBLP is applied THEN
	
	Maximum Authorized Bandwidth DL/UL per PDP Context is the sum of all Maximum
	Authorized Bandwidth DL/UL per media component for all the media component s
	to be carried by the PDP Context ;
	
	IF Maximum Authorized Bandwidth DL/UL per PDP Context > 2047 kbps THEN
	Maximum Authorized Bandwidth DL/UL per PDP Context = 2047 kbps /* See
	ref [8] */
	END;
	
	ELSE
	No authorization is done ;
	ENDIF ;

Maximum Authorized Traffic Class per PDP Context	IF SBLP is applied THEN
	
	Maximum Authorised Traffic Class per PDP Context = MAX [Maximum Authorised
	Traffic Class per media component among all the media component s to be
	carried by the PDP Context] ;
	
	ELSE
	No authorization is done ;
	ENDIF ;
	
	(The MAX function ranks the possible Maximum Authorised Traffic Class values as follows: Conversational > Streaming > Interactive > Background)

A.9.3 Mises en correspondance dans le GGSN (PEP)

Tableau A.13 Conversion attributs QdS IP autorisés - attributs QdS UMTS autorisés par le GGSN

Authorized UMTS QoS Parameter per PDP context	Derivation from Authorized IP QoS Parameters
Maximum Authorized Bandwidth DL and UL per PDP context	Maximum Authorized Bandwidth DL/UL per PDP context = Maximum Authorized Data Rate DL/UL per CLient Handle
Maximum Authorized Traffic Class per PDP context	IF Maximum Authorized QoS Class = "A" THEN Maximum Authorized Traffic Class = "Conversational" ELSEIF Maximum Authorized QoS Class = "B" THEN Maximum Authorized Traffic Class = "Streaming" ELSEIF Maximum Authorized QoS Class = "C" THEN Maximum Authorized Traffic Class = "Interactive" ELSEIF Maximum Authorized QoS Class = "D" THEN Maximum Authorized Traffic Class = "Interactive" ELSEIF Maximum Authorized QoS Class = "E" THEN Maximum Authorized Traffic Class = "Interactive" ELSE Maximum Authorized Traffic Class = "Background" ENDIF ;